Red Hat Directory Server 12

Configuring and managing replication

Replicating data to other Directory Server instances

Last Updated: 2024-04-29

Red Hat Directory Server 12 Configuring and managing replication

Replicating data to other Directory Server instances

Legal Notice

Abstract

To automatically synchronize data from one Directory Server instance to another, you can use a single supplier, multi supplier and cascading replication mechanism. To manage the replication changelog, you can use trimming and encryption.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For submitting feedback through Jira (account required):
  1. Log in to the Jira website.
  2. Click **Create** in the top navigation bar
  3. Enter a descriptive title in the **Summary** field.
  4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.
  5. Click **Create** at the bottom of the dialogue.
- For submitting feedback through Bugzilla (account required):
  1. Go to the Bugzilla website.
  2. As the Component, use **Documentation**.
  3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
  4. Click **Submit Bug**.

CHAPTER 1. CONFIGURING SINGLE-SUPPLIER REPLICATION USING THE COMMAND LINE

In a single-supplier replication environment, one writable supplier replicates data to one or multiple read-only consumers. For example, set up single-supplier replication if a suffix receives a large number of search requests but only a small number of write requests. To distribute the load, clients can then search for the suffix on read-only consumers and send write requests to the supplier.

This section assumes that you have an existing Directory Server instance running on a host named **supplier.example.com** that will act as a supplier in the replication topology to be set up. The procedures describe how to add a read-only consumer named **consumer.example.com** to the topology, and how to configure single-supplier replication for the **dc=example,dc=com** suffix.

1.1. PREPARING THE NEW CONSUMER USING THE COMMAND LINE

To prepare the **consumer.example.com** host, enable replication. This process:

- Configures the role of this server in the replication topology
- Defines the suffix that is replicated
- Creates the replication manager account the supplier uses to connect to this host

Perform this procedure on the consumer that you want to add to the replication topology.

Prerequisites

- You installed the Directory Server instance.
- The database for the **dc=example,dc=com** suffix exists.

Procedure

- Enable replication for the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldap://consumer.example.com replication enable
--suffix "dc=example,dc=com" --role "consumer" --bind-dn "cn=replication
manager,cn=config" --bind-passwd "password"
```

  This command configures the **consumer.example.com** host as a consumer for the **dc=example,dc=com** suffix. Additionally, the command creates the **cn=replication manager,cn=config** user with the specified password and allows this account to replicate changes for the suffix to this host.

Verification

- Display the replication configuration:

```
# dsconf -D "cn=Directory Manager" ldap://consumer.example.com replication get --
suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
```

```
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 2
...
```

These parameters indicate:

- **nsDS5ReplicaBindDN** specifies the replication manager account.
- **nsDS5ReplicaRoot** sets the suffix that is replicated.
- **nsDS5ReplicaType** set to **2** defines that this host is a consumer.

Additional resources

- Installing Red Hat Directory Server
- Storing suffixes in separate databases
- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

1.2. CONFIGURING THE EXISTING SERVER AS A SUPPLIER TO THE CONSUMER USING THE COMMAND LINE

To prepare the **supplier.example.com** host, you need to:

- Enable replication for the suffix.
- Create a replication agreement to the consumer.
- Initialize the consumer.

Perform this procedure on the existing supplier in the replication topology.

Prerequisites

- You enabled replication for the **dc=example,dc=com** suffix on the consumer.

Procedure

1. Enable replication for the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 1
```

This command configures the **supplier.example.com** host as a supplier for the **dc=example,dc=com** suffix, and sets the replica ID of this entry to **1**.

IMPORTANT

The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

2. Add the replication agreement and initialize the consumer:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt create --suffix "dc=example,dc=com" --host "consumer.example.com" --port 389 --conn-protocol=LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method=SIMPLE --init example-agreement
```

This command creates a replication agreement named **example-agreement**. The replication agreement defines settings, such as the consumer's host name, protocol, and authentication information that the supplier uses when connecting and replicating data to this consumer.

After the agreement was created, Directory Server initializes **consumer.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

1. Display the replication configuration:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication get --suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 3
...
```

These parameters indicate:

- **nsDS5ReplicaRoot** sets the suffix that is replicated.
- **nsDS5ReplicaType** set to **3** defines that this host is a supplier.

2. Verify whether the initialization was successful:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement
Agreement successfully initialized.
```

3. Display the replication status:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement
Status For Agreement: "example-agreement" (consumer.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210330075608Z
Last Update End: 20210330075608Z
Number Of Changes Sent: 1:3/0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210330074603Z
Last Init End: 20210330074606Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (6062d73c000000010000) consumer
```

```
(Unavailable) State (green) Reason (error (0) replica acquired successfully: incremental
update succeeded)
Replication Lag Time: Unavailable
```

Verify the **Replication Status** and **Last Update Status** fields.

Troubleshooting

1. By default, the replication idle timeout for all agreements on a server is 1 hour. If the initialization of large databases fails due to timeouts, set the **nsslapd-idletimeout** parameter to a higher value. For example, to set the parameter to **7200** (2 hours), enter:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com config replace
nsslapd-idletimeout=7200
```

To set an unlimited period, set **nsslapd-idletimeout** to **0**.

Additional resources

- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

CHAPTER 2. CONFIGURING SINGLE-SUPPLIER REPLICATION USING THE WEB CONSOLE

In a single-supplier replication environment, one writable supplier replicates data to one or multiple read-only consumers. For example, set up single-supplier replication if a suffix receives a large number of search requests but only a small number of write requests. To distribute the load, clients can then search for the suffix on read-only consumers and send write requests to the supplier.

This section assumes that you have an existing Directory Server instance running on a host named **supplier.example.com** that will act as a supplier in the replication topology to be set up. The procedures describe how to add a read-only consumer named **consumer.example.com** to the topology, and how to configure single-supplier replication for the **dc=example,dc=com** suffix.

2.1. PREPARING THE NEW CONSUMER USING THE WEB CONSOLE

To prepare the **consumer.example.com** host, enable replication. This process:

- Configures the role of this server in the replication topology
- Defines the suffix that is replicated
- Creates the replication manager account the supplier uses to connect to this host

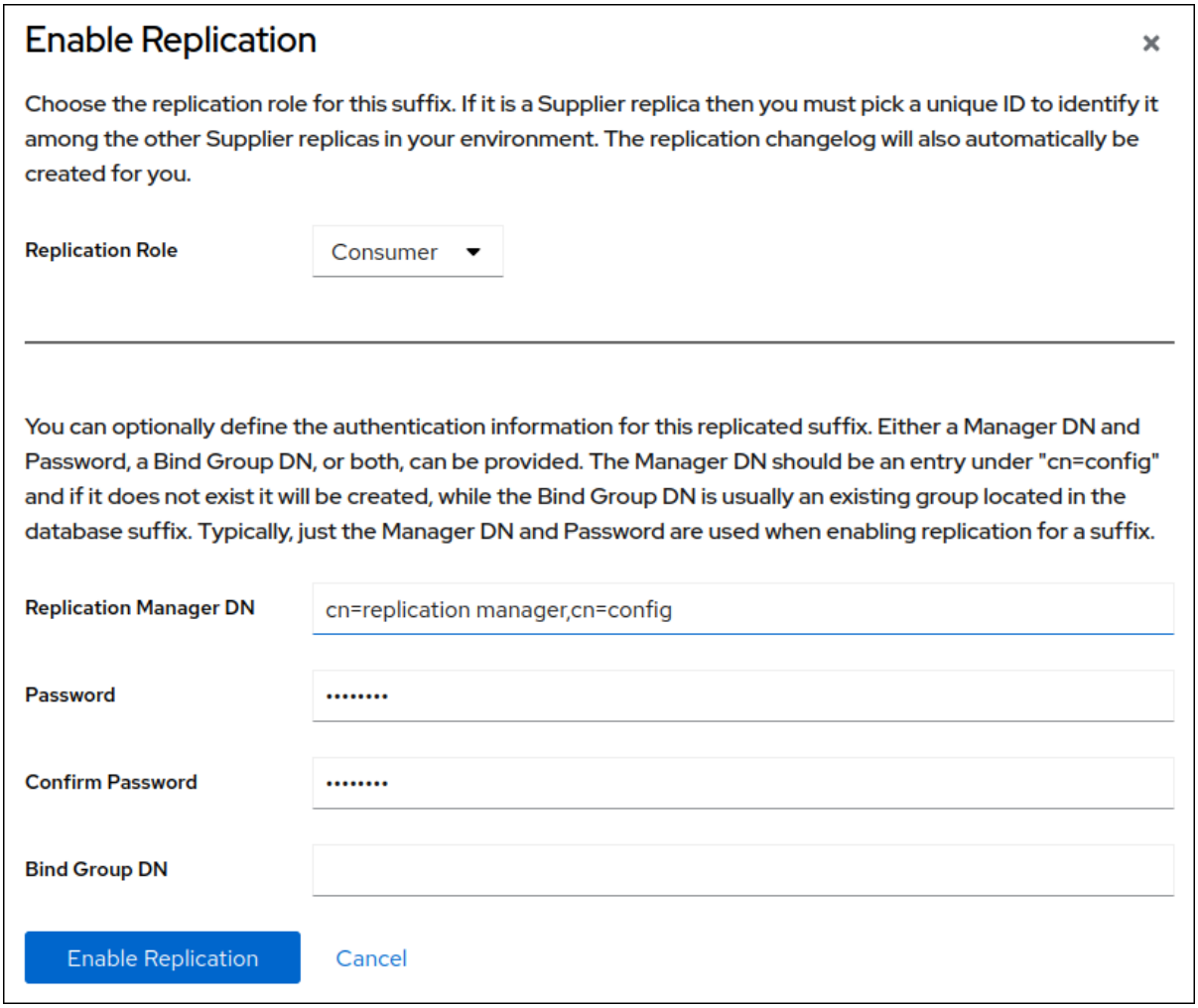
Perform this procedure on the consumer that you want to add to the replication topology.

Prerequisites

- You installed the Directory Server instance.
- The database for the **dc=example,dc=com** suffix exists.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Click **Enable Replication**.
4. Select **Consumer** in the **Replication Role** field, and enter the replication manager account and the password to create:



These settings configure the host as a consumer for the **dc=example,dc=com** suffix. Additionally, the server creates the **cn=replication manager,cn=config** user with the specified password and allows this account to replicate changes for the suffix to this host.

5. Click **Enable Replication**.

Verification

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. If the **Replica Role** field contains the value **Consumer**, replication is enabled, and the host is configured as a consumer.

Additional resources

- Installing Red Hat Directory Server
- Storing suffixes in separate databases

2.2. CONFIGURING THE EXISTING SERVER AS A SUPPLIER TO THE CONSUMER USING THE WEB CONSOLE

To prepare the **supplier.example.com** host, you need to:

- Enable replication for the suffix.
- Create a replication agreement to the consumer.
- Initialize the consumer.

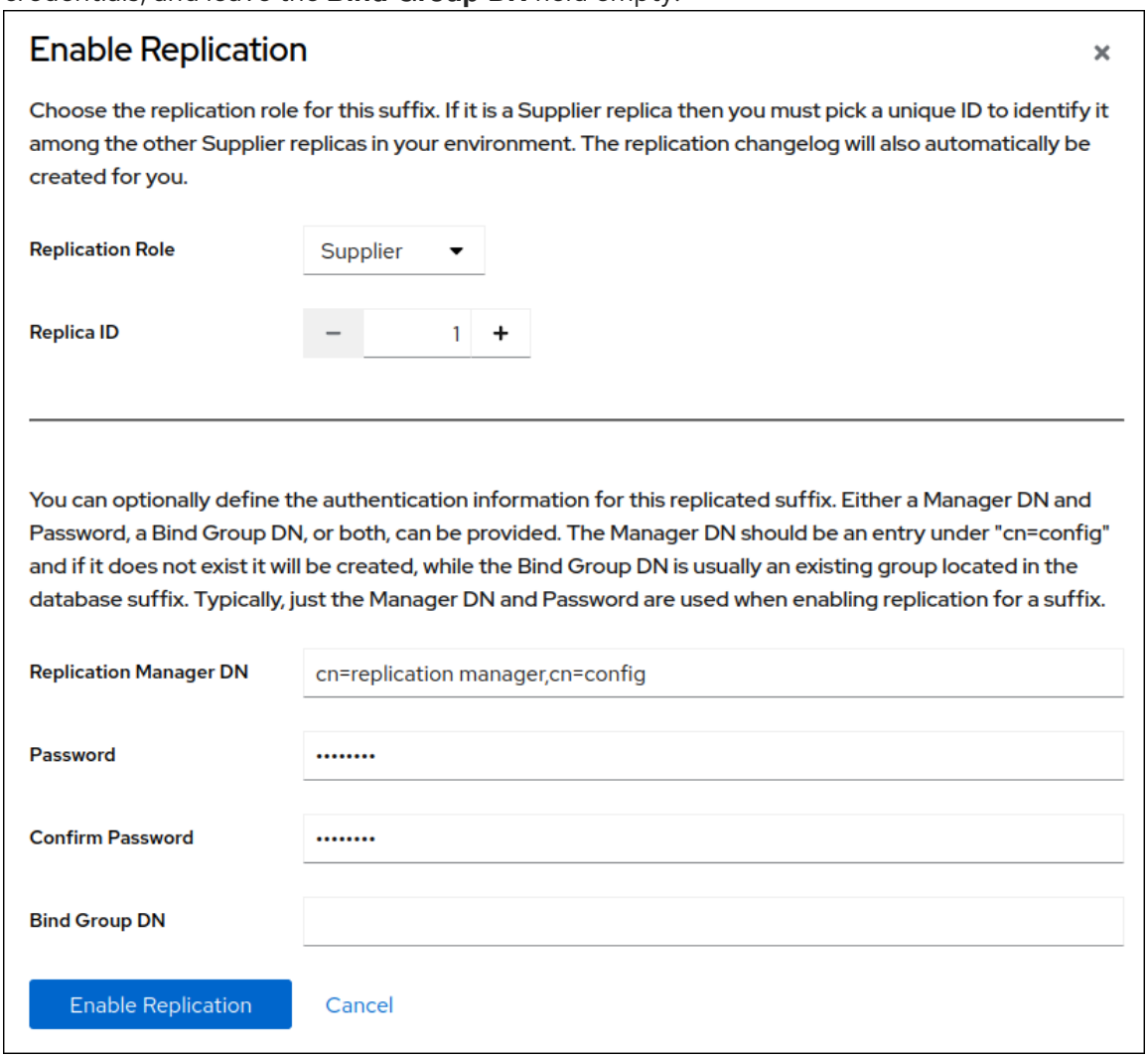
Perform this procedure on the existing supplier in the replication topology.

Prerequisites

- You enabled replication for the **dc=example,dc=com** suffix on the consumer.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Enable replication:
   a. Click **Enable Replication**.
   b. Select **Supplier** in the **Replication Role** field, enter a replica ID, replication manager credentials, and leave the **Bind Group DN** field empty:



These settings configure the host as a supplier for the **dc=example,dc=com** suffix and set the replica ID of this entry to **1**.

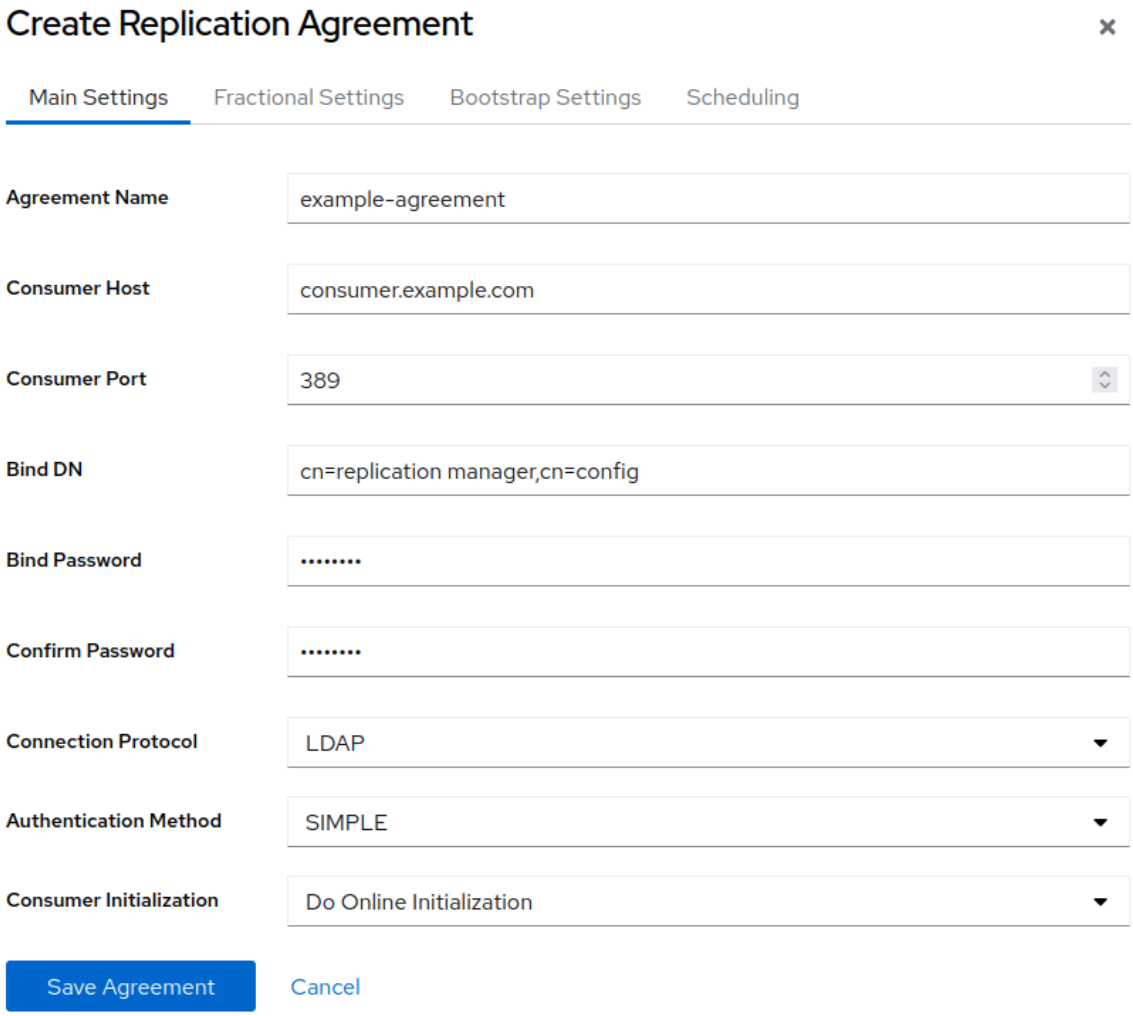
IMPORTANT

The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

c. Click **Enable Replication**.

4. Add a replication agreement and initialize the consumer:

a. On the **Agreements** tab, click **Create Agreement**, and fill the fields:



These settings create a replication agreement named **example-agreement**. The replication agreement defines settings, such as the consumer's host name, protocol, and authentication information that the supplier uses when connecting and replicating data to this consumer.

b. Select **Do Online Initialization** in the **Consumer Initialization** field to automatically initialize the consumer after saving the agreement.

c. Click **Save Agreement**.
After the agreement was created, Directory Server initializes **consumer.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. On the **Agreements** tab, verify the status of the agreement in the **State** column of the table.

CHAPTER 3. CONFIGURING MULTI-SUPPLIER REPLICATION USING THE COMMAND LINE

In a multi-supplier replication environment, two or more writable suppliers replicate data with each other. For example, set up multi-supplier replication to provide a fail-over environment and distribute the load over multiple servers. Clients can then perform read and write operations on any host that is a read-write replica.

This section assumes that you have an existing Directory Server instance running on a host named **supplier1.example.com**. The procedures describe how to add another read-write replica named **supplier2.example.com** to the topology, and how to configure multi-supplier replication for the **dc=example,dc=com** suffix.

3.1. PREPARING THE NEW SUPPLIER USING THE COMMAND LINE

To prepare the **supplier2.example.com** host, enable replication. This process:

- Configures the role of this server in the replication topology
- Defines the suffix that is replicated
- Creates the replication manager account the supplier uses to connect to this host

Perform this procedure on the supplier that you want to add to the replication topology.

Prerequisites

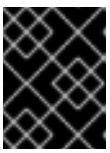
- You installed the Directory Server instance.
- The database for the **dc=example,dc=com** suffix exists.

Procedure

- Enable replication for the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 1 --bind-dn "cn=replication manager,cn=config" --bind-passwd "password"
```

This command configures the **supplier2.example.com** host as a supplier for the **dc=example,dc=com** suffix, and sets the replica ID of this entry to **1**. Additionally, the command creates the **cn=replication manager,cn=config** user with the specified password and allows this account to replicate changes for the suffix to this host.



IMPORTANT

The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

Verification

- Display the replication configuration:

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com replication get --
```

```
suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 3
...
```

These parameters indicate:

- **nsDS5ReplicaBindDN** specifies the replication manager account.
- **nsDS5ReplicaRoot** sets the suffix that is replicated.
- **nsDS5ReplicaType** set to **3** defines that this host is a supplier.

Additional resources

- Installing Red Hat Directory Server
- Storing suffixes in separate databases
- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

3.2. CONFIGURING THE EXISTING SERVER AS A SUPPLIER TO THE NEW SERVER USING THE COMMAND LINE

To prepare the existing server **supplier1.example.com** as a supplier, you need to:

- Enable replication for the suffix.
- Create a replication agreement to the new supplier.
- Initialize the new supplier.

Perform this procedure on the existing supplier in the replication topology.

Prerequisites

- You enabled replication for the **dc=example,dc=com** suffix on the supplier to join.

Procedure

1. Enable replication for the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 2 --bind-dn "cn=replication manager,cn=config" --bind-passwd "password"
```

This command configures the **supplier1.example.com** host as a supplier for the **dc=example,dc=com** suffix, and sets the replica ID of this entry to **2**. Additionally, the command creates the **cn=replication manager,cn=config** user with the specified password and allows this account to replicate changes for the suffix to this host.

IMPORTANT

The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

2. Add the replication agreement and initialize the new server:

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com repl-agmt create --suffix "dc=example,dc=com" --host "supplier2.example.com" --port 389 --conn-protocol LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method SIMPLE --init example-agreement-supplier1-to-supplier2
```

This command creates a replication agreement named **example-agreement-supplier1-to-supplier2**. The replication agreement defines settings, such as the new supplier's host name, protocol, and authentication information that the supplier uses when connecting and replicating data to the new supplier.

After the agreement was created, Directory Server initializes **supplier2.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

1. Display the replication configuration:

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com replication get --suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 3
...
```

These parameters indicate:

- **nsDS5ReplicaBindDN** specifies the replication manager account.
- **nsDS5ReplicaRoot** sets the suffix that is replicated.
- **nsDS5ReplicaType** set to **3** defines that this host is a supplier.

2. Verify whether the initialization was successful:

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement-supplier1-to-supplier2
Agreement successfully initialized.
```

3. Display the replication status:

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement-supplier1-to-supplier2
Status For Agreement: "example-agreement-supplier1-to-supplier2" (supplier2.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
```

```
Last Update Start: 20210331071545Z
Last Update End: 20210331071546Z
Number Of Changes Sent: 2:1/0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210331071541Z
Last Init End: 20210331071544Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (6064219e000100020000) consumer
(Unavailable) State (green) Reason (error (0) replica acquired successfully: incremental
update succeeded)
```

Verify the **Replication Status** and **Last Update Status** fields.

Troubleshooting

1. By default, the replication idle timeout for all agreements on a server is 1 hour. If the initialization of large databases fails due to timeouts, set the **nsslapd-idletimeout** parameter to a higher value. For example, to set the parameter to **7200** (2 hours), enter:

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com config replace
nsslapd-idletimeout=7200
```

To set an unlimited period, set **nsslapd-idletimeout** to **0**.

Additional resources

- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

3.3. CONFIGURING THE NEW SERVER AS A SUPPLIER TO THE EXISTING SERVER USING THE COMMAND LINE

To prepare the new server **supplier2.example.com** as a supplier, use either of the following methods:

- Enable replication for the suffix.
- Create a replication agreement to the existing server.

WARNING

Do not initialize the existing supplier from the new server. Otherwise, the empty database from the new server overrides the database on the existing supplier.

Apply the following procedure on the existing supplier:

- Create a replication agreement to the new server.
- Initialize the new server.

Prerequisites

- You enabled replication for the **dc=example,dc=com** suffix on the new server.
- You enabled replication for the **dc=example,dc=com** suffix on the existing server.
- The new server to join is successfully initialized.

Procedure

- Add the replication agreement to the existing instance:

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com repl-agmt create --suffix "dc=example,dc=com" --host "supplier1.example.com" --port 389 --conn-protocol LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method SIMPLE example-agreement-supplier2-to-supplier1
```

- Add the replication agreement to the new instance by using **--init** option:

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com repl-agmt create --suffix "dc=example,dc=com" --host "supplier2.example.com" --port 389 --conn-protocol LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method SIMPLE --init example-agreement-supplier1-to-supplier2
```

Verification

1. Display the agreement status:

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement-supplier2-to-supplier1
Agreement successfully initialized.
```

2. Display the replication status:

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement-supplier2-to-supplier1
Status For Agreement: ""example-agreement-supplier2-to-supplier1 (supplier1.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210331073540Z
Last Update End: 20210331073540Z
Number Of Changes Sent: 7:1/0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210331073535Z
Last Init End: 20210331073539Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (60642649000000070000) consumer (Unavailable) State (green) Reason (error (0) replica acquired successfully: incremental update succeeded)
Replication Lag Time: Unavailable
```

Verify the **Replication Status** and **Last Update Status** fields.

Troubleshooting

1. By default, the replication idle timeout for all agreements on a server is 1 hour. If the initialization of large databases fails due to timeouts, set the **nsslapd-idletimeout** parameter to a higher value. For example, to set the parameter to **7200** (2 hours), enter:

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com config replace
nsslapd-idletimeout=7200
```

   To set an unlimited period, set **nsslapd-idletimeout** to **0**.

CHAPTER 4. CONFIGURING MULTI-SUPPLIER REPLICATION USING THE WEB CONSOLE

In a multi-supplier replication environment, two or more writable suppliers replicate data with each other. For example, set up multi-supplier replication to provide a fail-over environment and distribute the load over multiple servers. Clients can then perform read and write operations on any host that is a read-write replica.

This section assumes that you have an existing Directory Server instance running on a host named **supplier1.example.com**. The procedures describe how to add another read-write replica named **supplier2.example.com** to the topology, and how to configure multi-supplier replication for the **dc=example,dc=com** suffix.

4.1. PREPARING THE NEW SUPPLIER USING THE WEB CONSOLE

To prepare the **supplier2.example.com** host, enable replication. This process:

- Configures the role of this server in the replication topology
- Defines the suffix that is replicated
- Creates the replication manager account the supplier uses to connect to this host

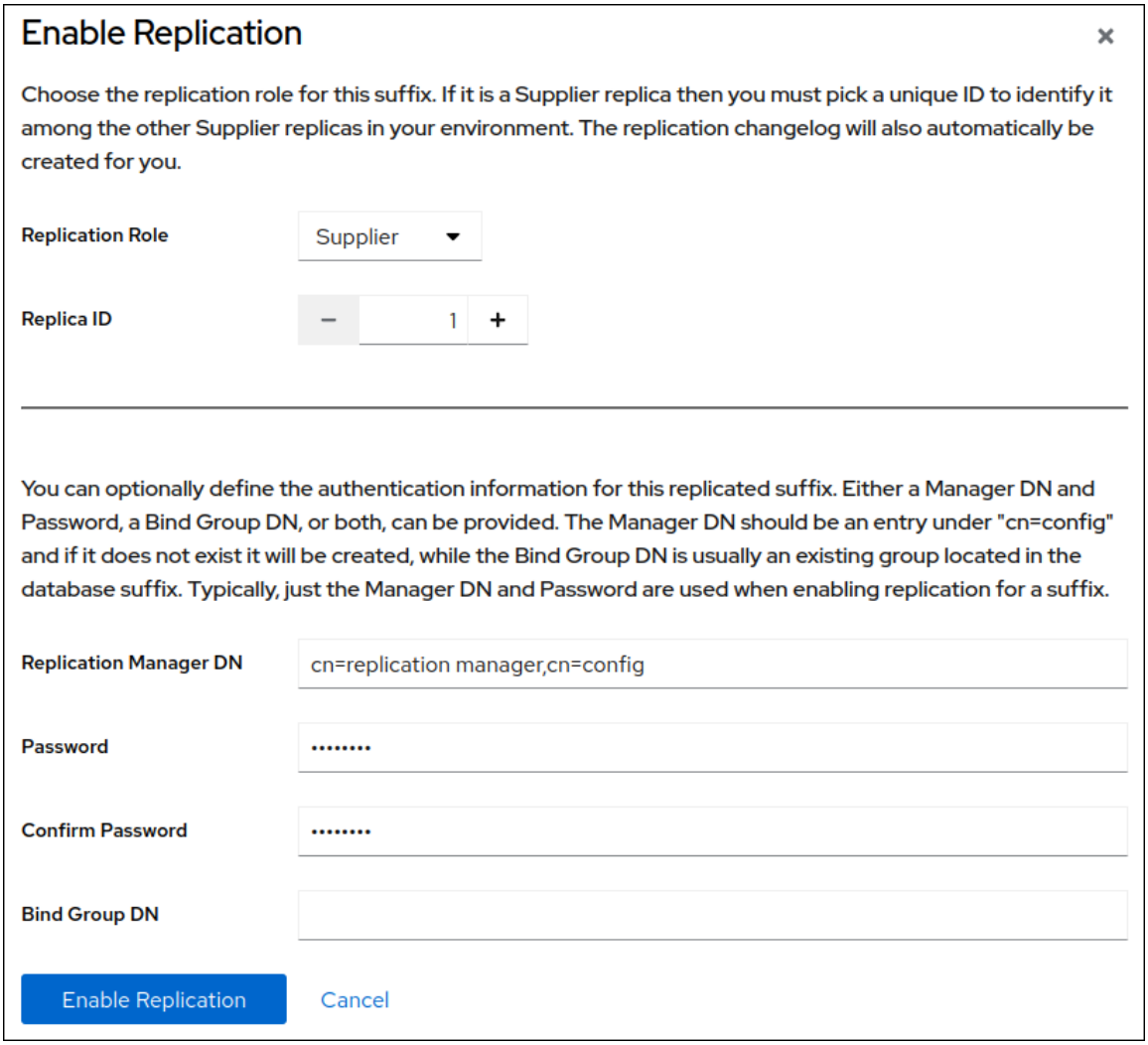
Perform this procedure on the supplier that you want to add to the replication topology.

Prerequisites

- You installed the Directory Server instance.
- The database for the **dc=example,dc=com** suffix exists.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Enable replication:
    a. Click **Enable Replication**.
    b. Select **Supplier** in the **Replication Role** field, enter a replica ID, as well as the distinguished name (DN) and password of the replication manager account to create:



These settings configure the host as a supplier for the **dc=example,dc=com** suffix and set the replica ID of this entry to **1**.

IMPORTANT

The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

If you set no replication manager DN, set a bind group DN. You can then use any member of this group in the replication agreement.

c. Click **Enable Replication**.

Verification

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. If the **Replica Role** field contains the value **Supplier**, replication is enabled, and the host is configured as a supplier.

Additional resources

- Installing Red Hat Directory Server

- Storing suffixes in separate databases

4.2. CONFIGURING THE EXISTING SERVER AS A SUPPLIER TO THE NEW SERVER USING THE WEB CONSOLE

To prepare the existing server **supplier1.example.com** as a supplier, you need to:

- Enable replication for the suffix.
- Create a replication agreement to the new supplier.
- Initialize the new supplier.

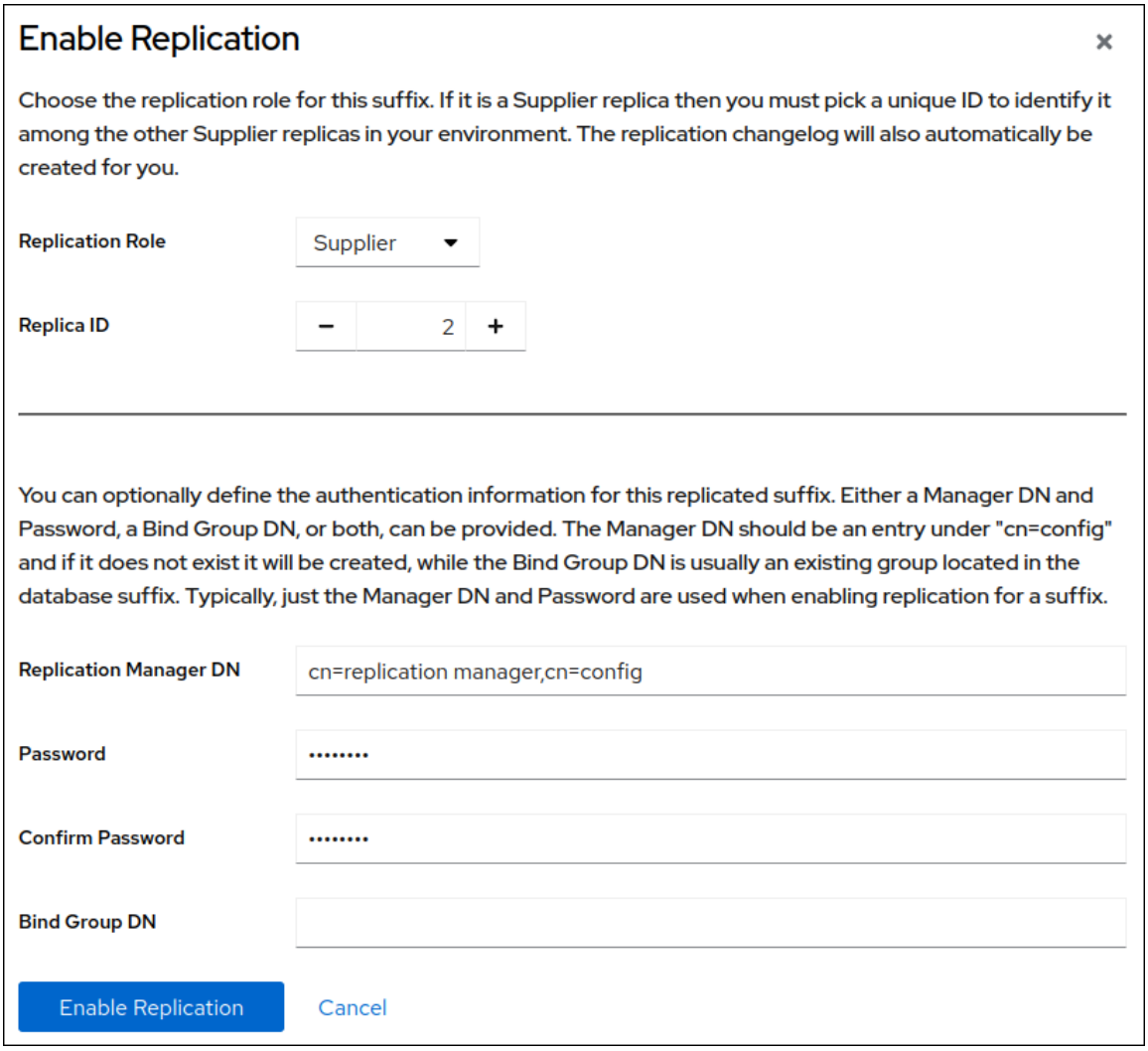
Perform this procedure on the existing supplier in the replication topology.

Prerequisites

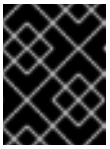
- You enabled replication for the **dc=example,dc=com** suffix on the supplier to join.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Enable replication:
   a. Click **Enable Replication**.
   b. Select **Supplier** in the **Replication Role** field, enter a replica ID, as well as the distinguished name (DN) and password of the replication manager account to create:



These settings configure the host as a supplier for the **dc=example,dc=com** suffix and set the replica ID of this entry to **2**.



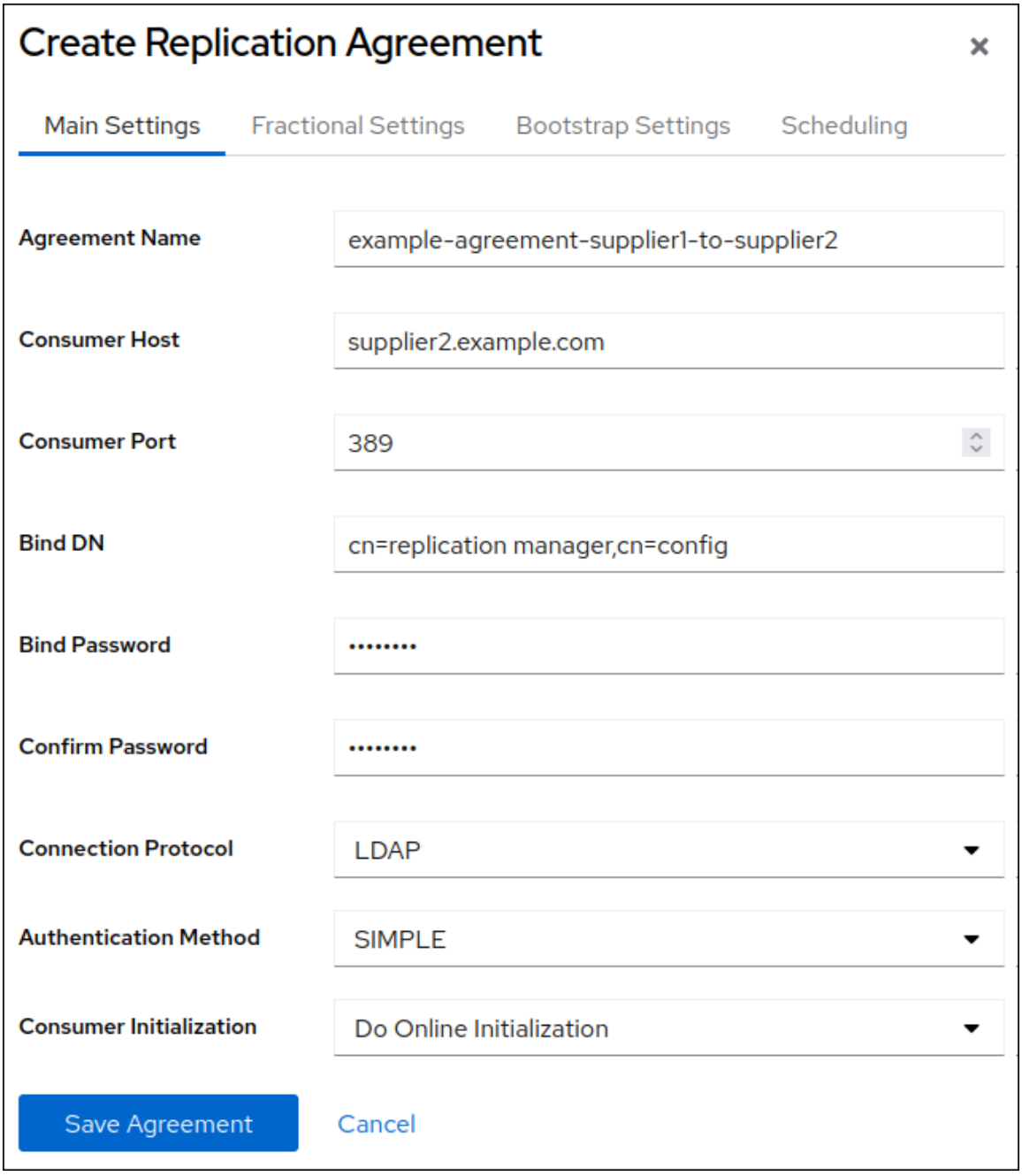
IMPORTANT

The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

c. Click **Enable Replication**.

4. Add a replication agreement and initialize the new server:

a. On the **Agreements** tab, click **Create Agreement**, and fill the fields:



These settings create a replication agreement named **example-agreement-supplier1-to-supplier2**. The replication agreement defines settings, such as the new supplier's host name, protocol, and authentication information that the supplier uses when connecting and replicating data to the new supplier.

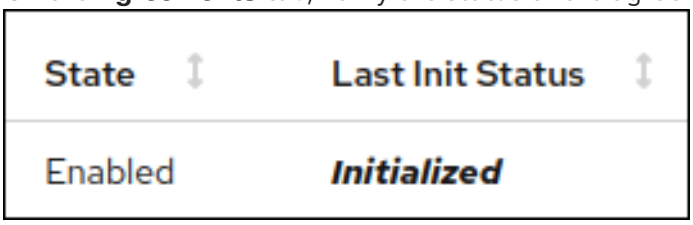
b. Select **Do Online Initialization** in the **Consumer Initialization** field to automatically initialize the new server after saving the agreement.

c. Click **Save Agreement**.
After the agreement was created, Directory Server initializes **supplier2.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.

3. On the **Agreements** tab, verify the status of the agreement in the **State** column of the table.



4.3. CONFIGURING THE NEW SERVER AS A SUPPLIER TO THE EXISTING SERVER USING THE WEB CONSOLE

To prepare the new server **supplier2.example.com** as a supplier, you need to:

- Enable replication for the suffix.
- Create a replication agreement to the existing server.
- Initialize the existing server.

Perform this procedure on the existing supplier in the replication topology.

WARNING

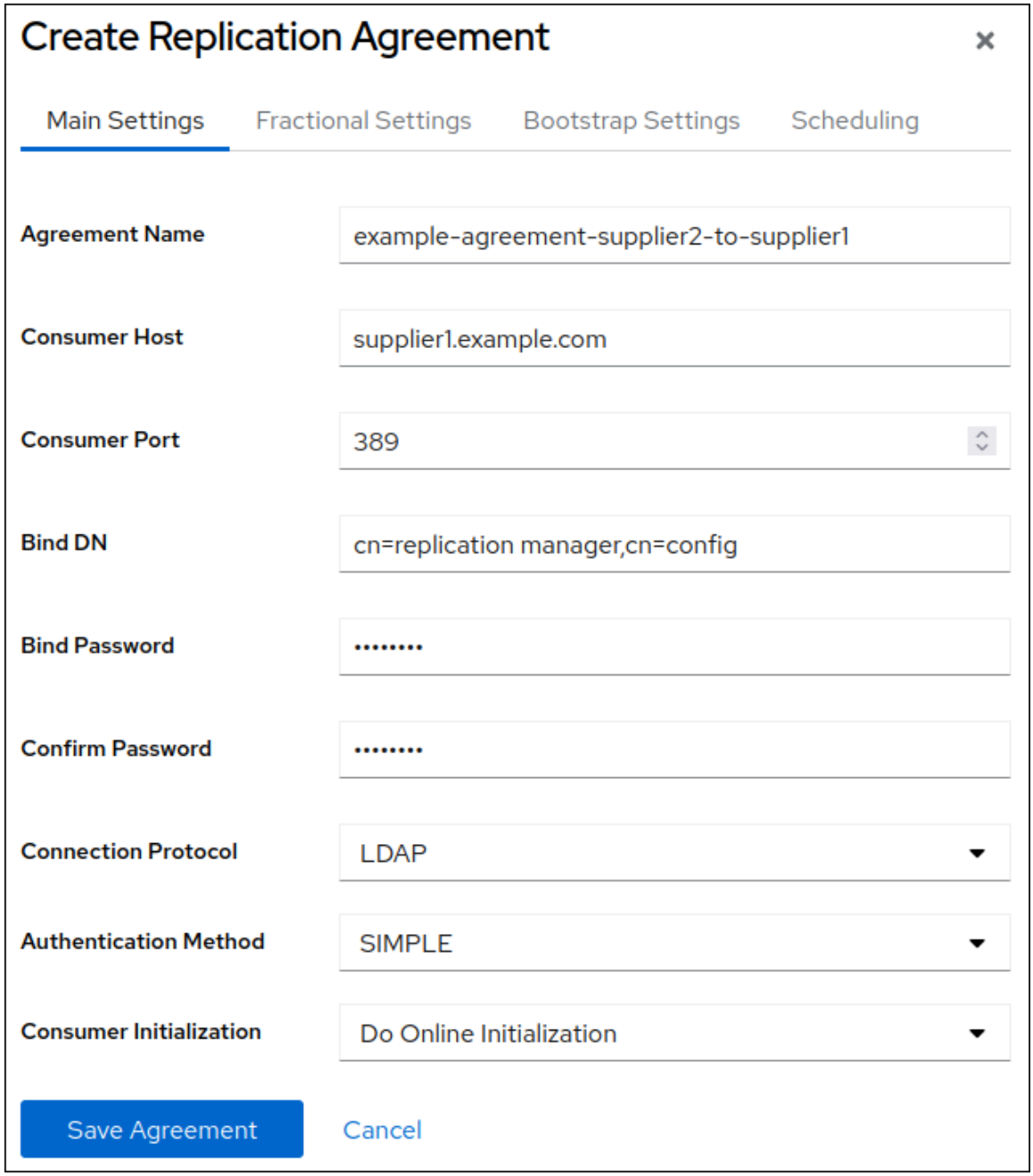
Do not continue if you have not initialized the replication agreement on the existing server. Otherwise, the empty database from the new server overrides the database on the existing supplier.

Prerequisites

- You enabled replication for the **dc=example,dc=com** suffix on the new server.
- You enabled replication for the **dc=example,dc=com** suffix on the existing server.
- The new server to join is successfully initialized.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Add a replication agreement and initialize the existing server:
    a. On the **Agreements** tab, click **Create Agreement**, and fill the fields:



These settings create a replication agreement named **example-agreement-supplier2-to-supplier1**. The replication agreement defines settings, such as the existing server's host name, protocol, and authentication information that the supplier uses when connecting and replicating data to the existing supplier.

b. Select **Do Online Initialization** in the **Consumer Initialization** field to automatically initialize the new server after saving the agreement.

c. Click **Save Agreement**.
After the agreement was created, Directory Server initializes **supplier1.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. On the **Agreements** tab, verify the status of the agreement in the **State** column of the table.


State
Last Init Status
Enabled
Initialized

CHAPTER 5. CONFIGURING MULTI-SUPPLIER REPLICATION WITH CERTIFICATE-BASED AUTHENTICATION

When you set up replication between two Directory Server instances, you can use certificate-based authentication instead of using a bind DN and password to authenticate to a replication partner.

You can do so by adding a new server to the replication topology and setting up replication agreements between the new host and the existing server using certificate-based authentication.

IMPORTANT

Certificate-based authentication requires TLS-encrypted connections.

5.1. PREPARING ACCOUNTS AND A BIND GROUP FOR THE USE IN REPLICATION AGREEMENTS WITH CERTIFICATE-BASED AUTHENTICATION

To use certificate-based authentication in replication agreements, first prepare the accounts and store the client certificates in the **userCertificate** attributes of these accounts. Additionally, this procedure creates a bind group that you later use in the replication agreements.

Perform this procedure on the existing host **server1.example.com**.

Prerequisites

- You enabled TLS encryption in Directory Server.
- You stored the client certificates in distinguished encoding rules (DER) format in the **/root/server1.der** and **/root/server2.der** files.
  For details about client certificates and how to request them from your certificate authority (CA), see your CA's documentation.

Procedure

1. Create the **ou=services** entry if it does not exist:

```
# ldapadd -D "cn=Directory Manager" -W -H ldaps://server1.example.com -x

dn: ou=services,dc=example,dc=com
objectClass: organizationalunit
objectClass: top
ou: services
```

2. Create accounts for both servers, such as **cn=server1,ou=services,dc=example,dc=com** and **cn=server1,ou=services,dc=example,dc=com**:

```
# ldapadd -D "cn=Directory Manager" -W -H ldaps://server1.example.com -x

dn: cn=server1,ou=services,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: inetOrgPerson
sn: server1
```

```
cn: server1
userPassword: password
userCertificate:< file:///root/server1.der

adding new entry "cn=server1,ou=services,dc=example,dc=com"

dn: cn=server2,ou=services,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: inetOrgPerson
sn: server2
cn: server2
userPassword: password
userCertificate:< file:///root/server2.der

adding new entry "cn=server2,ou=services,dc=example,dc=com"
```

3. Create a group, such as **cn=repl_servers,dc=groups,dc=example,dc=com**:

```
# dsidm -D "cn=Directory Manager" ldaps://server1.example.com -b
"dc=example,dc=com" group create --cn "repl_servers"
```

4. Add the two replication accounts as members to the group:

```
# dsidm -D "cn=Directory Manager" ldaps://server1.example.com -b
"dc=example,dc=com" group add_member repl_servers
"cn=server1,ou=services,dc=example,dc=com"

# dsidm -D "cn=Directory Manager" ldaps://server1.example.com -b
"dc=example,dc=com" group add_member repl_servers
"cn=server2,ou=services,dc=example,dc=com"
```

Additional resources

- Enabling TLS-encrypted connections to Directory Server

5.2. INITIALIZING A NEW SERVER USING A TEMPORARY REPLICATION MANAGER ACCOUNT

Certificate-based authentication uses the certificates stored in the directory. However, before you initialize a new server, the database on **server2.example.com** is empty and the accounts with the associated certificates do not exist. Therefore, replication using certificates is not possible before the database is initialized. You can overcome this problem by initializing **server2.example.com** with a temporary replication manager account.

Prerequisites

- You installed the Directory Server instance on **server2.example.com**.
- The database for the **dc=example,dc=com** suffix exists.
- You enabled TLS encryption in Directory Server on both servers, **server1.example.com** and **server2.example.com**.

Procedure

1. On **server2.example.com**, enable replication for the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldaps://server2.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 2 --bind-dn "cn=replication manager,cn=config" --bind-passwd "password"
```

   This command configures the **server2.example.com** host as a supplier for the **dc=example,dc=com** suffix, and sets the replica ID of this host to **2**. Additionally, the command creates a temporary **cn=replication manager,cn=config** user with the specified password and allows this account to replicate changes for the suffix to this host.

   The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

2. On **server1.example.com**:

   a. Enable replication:

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com replication enable --suffix="dc=example,dc=com" --role="supplier" --replica-id="1"
```

   b. Create a temporary replication agreement which uses the temporary account from the previous step for authentication:

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt create --suffix="dc=example,dc=com" --host="server1.example.com" --port=636 --conn-protocol=LDAPS --bind-dn="cn=Replication Manager,cn=config" --bind-passwd="password" --bind-method=SIMPLE --init temporary_agreement
```

Verification

1. Verify that the initialization was successful:

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt init-status --suffix "dc=example,dc=com" temporary_agreement
Agreement successfully initialized.
```

Additional resources

- Installing Red Hat Directory Server
- Enabling TLS-encrypted connections to Directory Server

5.3. CONFIGURING MULTI-SUPPLIER REPLICATION WITH CERTIFICATE-BASED AUTHENTICATION

In a multi-supplier replication environment with certificate-based authentication, the replicas authenticate each others using certificates.

Prerequisites

- You set up certificate-based authentication on both hosts, **server1.example.com** and **server2.example.com**.
- Directory Server trusts the certificate authority (CA) that issues the client certificates.
- The client certificates meet the requirements set in **/etc/dirsrv/slapd-instance_name/certmap.conf** on the servers.

Procedure

1. On **server1.example.com**:
   a. Remove the temporary replication agreement:

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt delete
--suffix="dc=example,dc=com" temporary_agreement
```

   b. Add the **cn=repl_servers,dc=groups,dc=example,dc=com** bind group to the replication settings:

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com replication set --
suffix="dc=example,dc=com" --repl-bind-group
"cn=repl_servers,dc=groups,dc=example,dc=com"
```

   c. Configure Directory Server to automatically check for changes in the bind group:

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com replication set --
suffix="dc=example,dc=com" --repl-bind-group-interval=0
```

2. On **server2.example.com**:
   a. Remove the temporary replication manager account:

```
# dsconf -D "cn=Directory Manager" ldaps://server2.example.com replication
delete-manager --suffix="dc=example,dc=com" --name="Replication Manager"
```

   b. Add the **cn=repl_servers,dc=groups,dc=example,dc=com** bind group to the replication settings:

```
# dsconf -D "cn=Directory Manager" ldaps://server2.example.com replication set --
suffix="dc=example,dc=com" --repl-bind-group
"cn=repl_servers,dc=groups,dc=example,dc=com"
```

   c. Configure Directory Server to automatically check for changes in the bind group:

```
# dsconf -D "cn=Directory Manager" ldap://server2.example.com replication set --
suffix="dc=example,dc=com" --repl-bind-group-interval=0
```

   d. Create the replication agreement with certificate-based authentication:

```
dsconf -D "cn=Directory Manager" ldaps://server2.example.com repl-agmt create --
suffix="dc=example,dc=com" --host="server1.example.com" --port=636 --conn-
protocol=LDAPS --bind-method="SSLCLIENTAUTH" --init server2-to-server1
```

3. On **server1.example.com**, create the replication agreement with certificate-based authentication:

```
dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt create --
suffix="dc=example,dc=com" --host="server2.example.com" --port=636 --conn-
protocol=LDAPS --bind-method="SSLCLIENTAUTH" --init server1-to-server2
```

Verification

1. Verify on each server that the initialization was successful:

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt init-status
--suffix "dc=example,dc=com" server1-to-server2
Agreement successfully initialized.

# dsconf -D "cn=Directory Manager" ldaps://server2.example.com repl-agmt init-status
--suffix "dc=example,dc=com" server2-to-server1
Agreement successfully initialized.
```

Additional resources

- Setting up certificate-based authentication
- Changing the CA trust flags

CHAPTER 6. CONFIGURING CASCADING REPLICATION USING THE COMMAND LINE

In a cascading replication scenario, one server, a hub, acts both as a consumer and a supplier. The hub is a read-only replica that maintains a changelog. It receives updates from the supplier and supplies these updates to a consumer. Use cascading replication for balancing heavy traffic loads or to keep suppliers based locally in geographically-distributed environments.

6.1. PREPARING THE NEW HUB SERVER USING THE COMMAND LINE

To prepare the **hub.example.com** host, enable replication. This process:

- Configures the role of this server in the replication topology
- Defines the suffix that is replicated
- Creates the replication manager account the supplier uses to connect to this host

Perform this procedure on the hub that you want to add to the replication topology.

Prerequisites

- You installed the Directory Server instance.
- The database for the dc=example,dc=com suffix exists.

Procedure

- Enable replication for the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com replication enable --suffix "dc=example,dc=com" --role "hub" --bind-dn "cn=replication manager,cn=config" --bind-passwd "password"
```

This command configures the **hub.example.com** host as a hub for the **dc=example,dc=com** suffix. Additionally, the command creates the **cn=replication manager,cn=config** user with the specified password and allows this account to replicate changes for the suffix to this host.

Verification

- Display the replication configuration:

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com replication get --suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 2
nsDS5ReplicaId: 65535
...
```

These parameters indicate:

- **nsDS5ReplicaBindDN** specifies the replication manager account.
- **nsDS5ReplicaRoot** sets the suffix that is replicated.
- **nsDS5ReplicaType** set to **2** defines that this host is a consumer, which is also valid for a hub.
- **nsDS5ReplicaId** set to **65535** defines that this host is a hub. The **dsconf** utility automatically sets this value if you define the **--role "hub"** option.

Additional resources

- Installing Red Hat Directory Server
- Storing suffixes in separate databases
- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

6.2. CONFIGURING THE EXISTING SERVER AS A SUPPLIER TO THE HUB SERVER USING THE COMMAND LINE

To prepare the existing server as a supplier, you need to:

- Enable replication for the suffix.
- Create a replication agreement to the hub.
- Initialize the hub.

Perform this procedure on the existing supplier in the replication topology.

Prerequisites

- You enabled replication for the **dc=example,dc=com** suffix on the hub to join.

Procedure

1. Enable replication for the **dc=example,dc=com** suffix:

```
# [command]`dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 1
```

This command configures the **supplier.example.com** host as a supplier for the **dc=example,dc=com** suffix, and sets the replica ID of this entry to **1**.

IMPORTANT

The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

2. Add the replication agreement and initialize the new server:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt create --suffix "dc=example,dc=com" --host "hub.example.com" --port 389 --conn-protocol
```

```
LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --
bind-method SIMPLE --init example-agreement-supplier-to-hub
```

This command creates a replication agreement named **example-agreement-supplier-to-hub**. The replication agreement defines settings, such as the hub's host name, protocol, and authentication information that the supplier uses when connecting and replicating data to the hub.

After the agreement was created, Directory Server initializes **hub.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

1. Display the replication configuration:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication get --
suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 3
...
```

These parameters indicate:

- **nsDS5ReplicaRoot** sets the suffix that is replicated.
- **nsDS5ReplicaType** set to **3** defines that this host is a supplier.

2. Verify whether the initialization was successful:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt init-status
--suffix "dc=example,dc=com" example-agreement-supplier-to-hub
Agreement successfully initialized.
```

3. Display the replication status:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt status --
suffix "dc=example,dc=com" example-agreement-supplier-to-hub
Status For Agreement: "example-agreement-supplier-to-hub" (hub.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210331105030Z
Last Update End: 20210331105030Z
Number Of Changes Sent: 0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210331105026Z
Last Init End: 20210331105029Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (Unknown) consumer (Unknown) State
(green) Reason (error (0) replica acquired successfully: incremental update succeeded)
Replication Lag Time: Unavailable
```

Verify the **Replication Status** and **Last Update Status** fields.

Troubleshooting

1. By default, the replication idle timeout for all agreements on a server is 1 hour. If the initialization of large databases fails due to timeouts, set the **nsslapd-idletimeout** parameter to a higher value. For example, to set the parameter to **7200** (2 hours), enter:

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com config replace
nsslapd-idletimeout=7200
```

   To set an unlimited period, set **nsslapd-idletimeout** to **0**.

Additional resources

- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

6.3. PREPARING THE NEW CONSUMER OF THE HUB USING THE COMMAND LINE

To prepare the **consumer.example.com** host, enable replication. This process:

- Configures the role of this server in the replication topology
- Defines the suffix that is replicated
- Creates the replication manager account the hub uses to connect to this host

Perform this procedure on the consumer that you want to add to the replication topology.

Prerequisites

- You installed the Directory Server instance.
- The database for the **dc=example,dc=com** suffix exists.

Procedure

- Enable replication for the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldap://consumer.example.com replication enable
--suffix "dc=example,dc=com" --role "consumer" --bind-dn "cn=replication
manager,cn=config" --bind-passwd "password"
```

  This command configures the **consumer.example.com** host as a consumer for the **dc=example,dc=com** suffix. Additionally, the command creates the **cn=replication manager,cn=config** user with the specified password and allows this account to replicate changes for the suffix to this host.

Verification

- Display the replication configuration:

```
# dsconf -D "cn=Directory Manager" ldap://consumer.example.com replication get --
```

```
suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 2
...
```

These parameters indicate:

- **nsDS5ReplicaBindDN** specifies the replication manager account.
- **nsDS5ReplicaRoot** sets the suffix that is replicated.
- **nsDS5ReplicaType** set to **2** defines that this host is a consumer.

Additional resources

- Installing Red Hat Directory Server
- Storing suffixes in separate databases
- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

6.4. CONFIGURING THE HUB SERVER AS A SUPPLIER FOR THE CONSUMER USING THE COMMAND LINE

To prepare the hub, you need to:

- Create a replication agreement to the consumer.
- Initialize the consumer.

Perform this procedure on the hub in the replication topology.

Prerequisites

- The hub is initialized, and replication from the supplier to the hub works.
- You enabled replication for the **dc=example,dc=com** suffix on the hub.

Procedure

- Add the replication agreement and initialize the consumer:

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com repl-agmt create --suffix
"dc=example,dc=com" --host "consumer.example.com" --port 389 --conn-protocol
LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --
bind-method SIMPLE --init example-agreement-hub-to-consumer
```

This command creates a replication agreement named **example-agreement-hub-to-consumer**. The replication agreement defines settings, such as the consumer's host name, protocol, and authentication information that the supplier uses when connecting and replicating data to this consumer.

After the agreement was created, Directory Server initializes **consumer.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

1. Verify whether the initialization was successful:

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement-hub-to-consumer
Agreement successfully initialized.
```

2. Display the replication status:

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement-hub-to-consumer
Status For Agreement: "example-agreement-hub-to-consumer" (consumer.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210331131534Z
Last Update End: 20210331131534Z
Number Of Changes Sent: 0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210331131530Z
Last Init End: 20210331131533Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (Unknown) consumer (Unknown) State (green) Reason (error (0) replica acquired successfully: incremental update succeeded)
Replication Lag Time: Unavailable
```

Verify the **Replication Status** and **Last Update Status** fields.

Troubleshooting

1. By default, the replication idle timeout for all agreements on a server is 1 hour. If the initialization of large databases fails due to timeouts, set the **nsslapd-idletimeout** parameter to a higher value. For example, to set the parameter to **7200** (2 hours), enter:

```
# dsconf -D "cn=Directory Manager" ldap://hub .example.com config replace nsslapd-idletimeout=7200
```

To set an unlimited period, set **nsslapd-idletimeout** to **0**.

CHAPTER 7. CONFIGURING CASCADING REPLICATION USING THE WEB CONSOLE

In a cascading replication scenario, one server, a hub, acts both as a consumer and a supplier. The hub is a read-only replica that maintains a changelog. It receives updates from the supplier and supplies these updates to a consumer. Use cascading replication for balancing heavy traffic loads or to keep suppliers based locally in geographically-distributed environments.

7.1. PREPARING THE NEW HUB SERVER USING THE WEB CONSOLE

To prepare the **hub.example.com** host, enable replication. This process:

- Configures the role of this server in the replication topology
- Defines the suffix that is replicated
- Creates the replication manager account the supplier uses to connect to this host

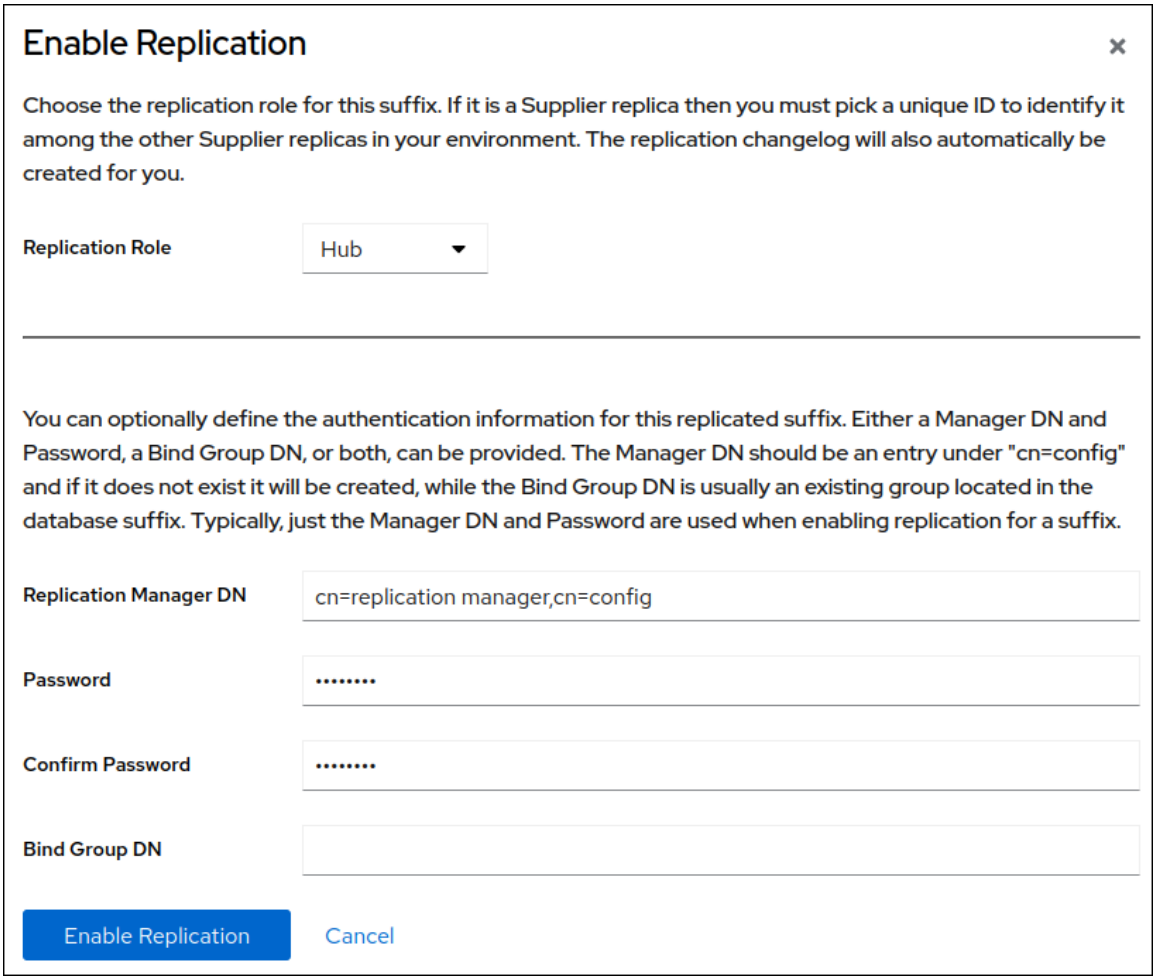
Perform this procedure on the hub that you want to add to the replication topology.

Prerequisites

- You installed the Directory Server instance.
- The database for the dc=example,dc=com suffix exists.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Enable replication:
    a. Click **Enable Replication**.
    b. Select **Consumer** in the **Replication Role** field, and enter the replication manager account and the password to create:



These settings configure the host as a hub for the **dc=example,dc=com** suffix.

c. Click **Enable Replication**.

Verification

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. If the **Replica Role** field contains the value **Hub**, replication is enabled, and the host is configured as a consumer.

Additional resources

- Installing Red Hat Directory Server
- Storing suffixes in separate databases

7.2. CONFIGURING THE EXISTING SERVER AS A SUPPLIER TO THE HUB SERVER USING THE WEB CONSOLE

To prepare the existing server as a supplier, you need to:

- Enable replication for the suffix.
- Create a replication agreement to the hub.

- Initialize the hub.

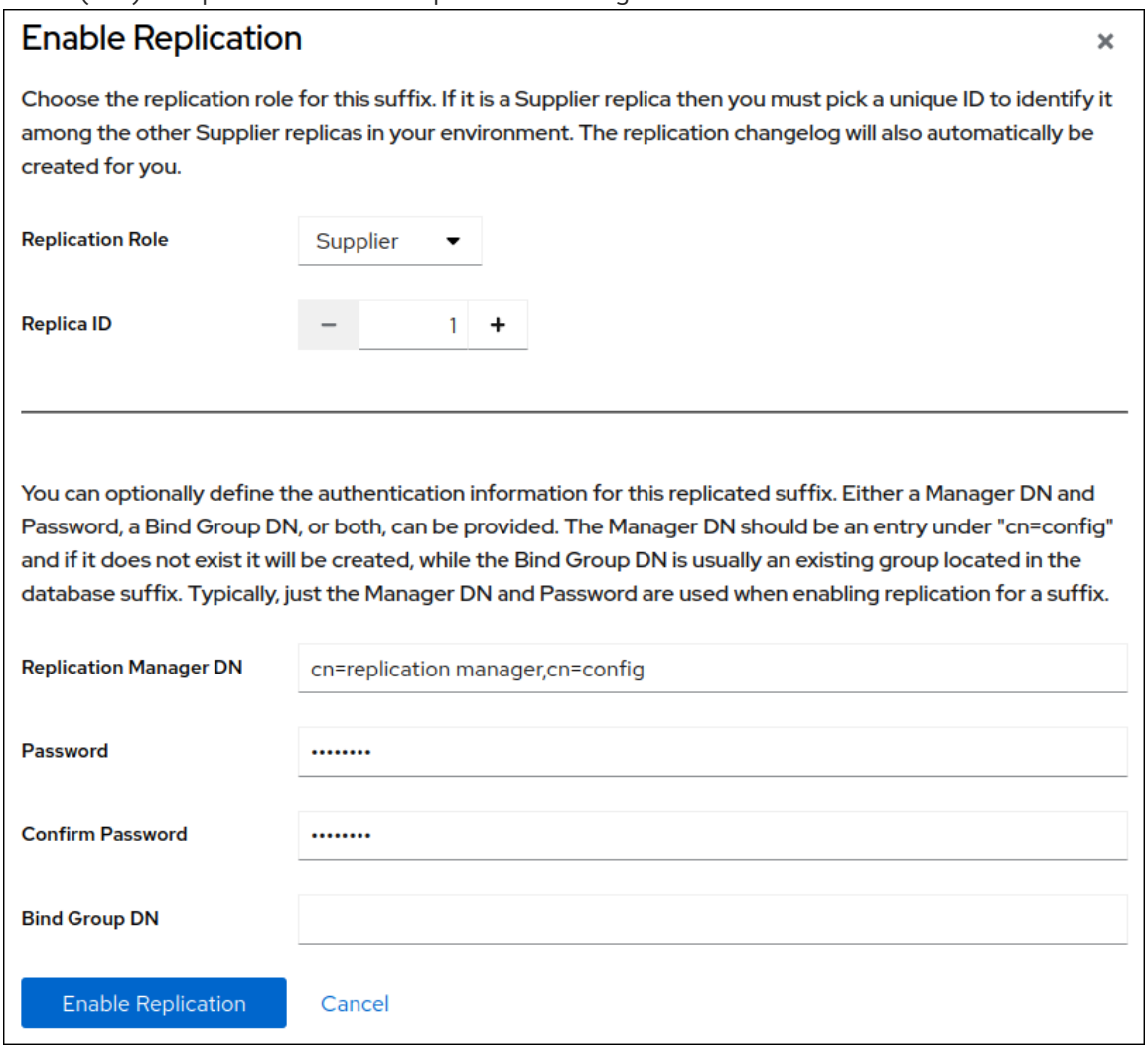
Perform this procedure on the existing supplier in the replication topology.

Prerequisites

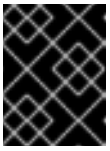
- You enabled replication for the **dc=example,dc=com** suffix on the hub to join.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Enable replication:
   a. Click **Enable Replication**.
   b. Select **Supplier** in the **Replication Role** field, enter a replica ID, as well as the distinguished name (DN) and password of the replication manager account to create:



These settings configure the host as a supplier for the **dc=example,dc=com** suffix and set the replica ID of this entry to **1**.



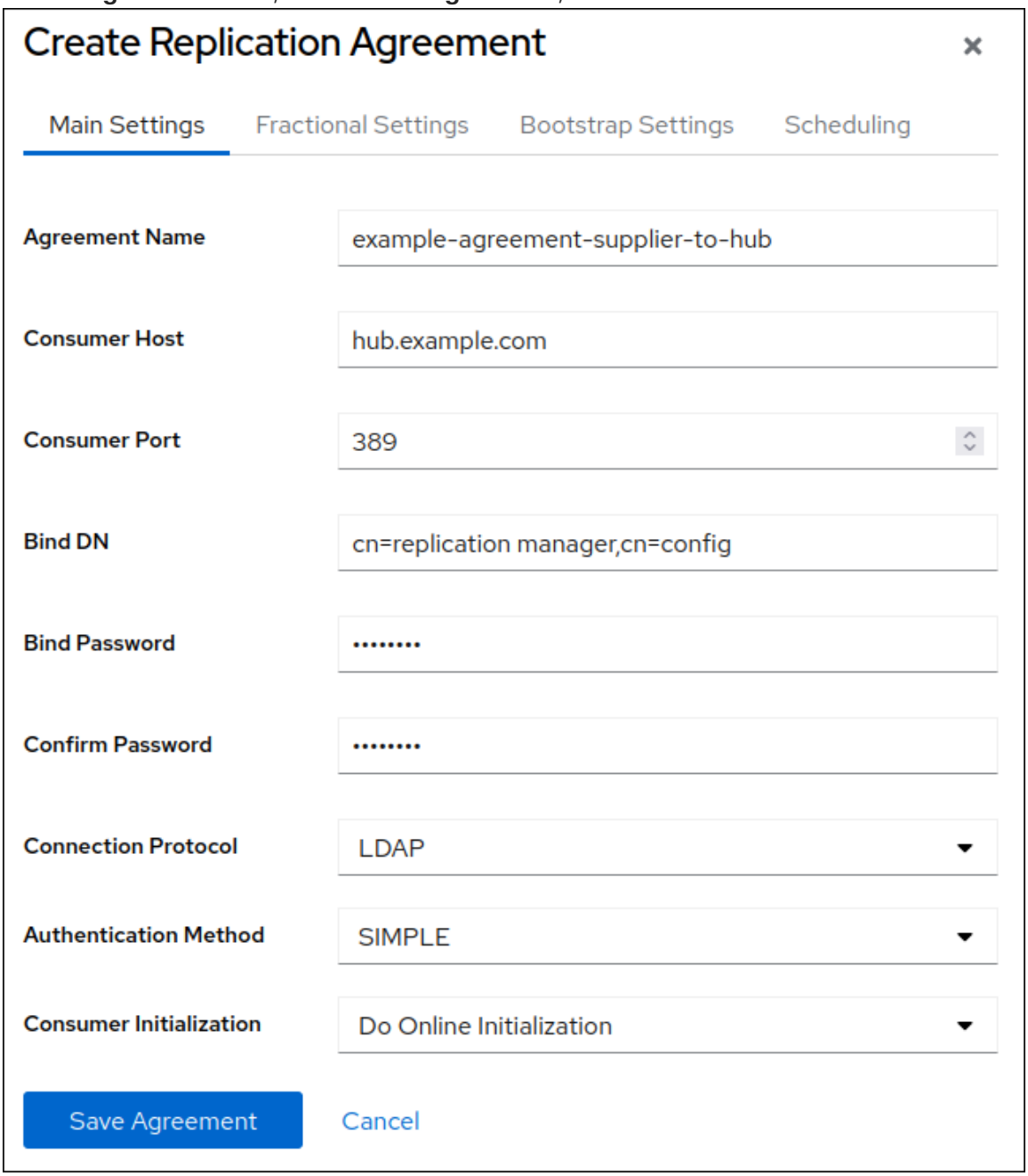
IMPORTANT

The replica ID must be a unique integer between **1** and **65534** for a suffix across all suppliers in the topology.

c. Click **Enable Replication**.

4. Add a replication agreement and initialize the new server:

a. On the **Agreements** tab, click **Create Agreement**, and fill the fields:



These settings create a replication agreement named **example-agreement-supplier-to-hub**. The replication agreement defines settings, such as the hub's host name, protocol, and authentication information that the supplier uses when connecting and replicating data to this hub.

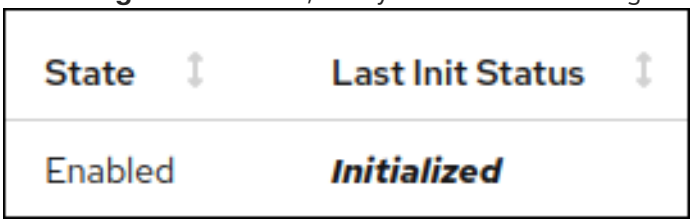
b. Select **Do Online Initialization** in the **Consumer Initialization** field to automatically initialize the new server after saving the agreement.

c. Click **Save Agreement**.

After the agreement was created, Directory Server initializes **hub.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. On the **Agreements** tab, verify the status of the agreement in the **State** column of the table.



7.3. PREPARING THE NEW CONSUMER OF THE HUB USING THE WEB CONSOLE

To prepare the **consumer.example.com** host, enable replication. This process:

- Configures the role of this server in the replication topology
- Defines the suffix that is replicated
- Creates the replication manager account the supplier uses to connect to this host

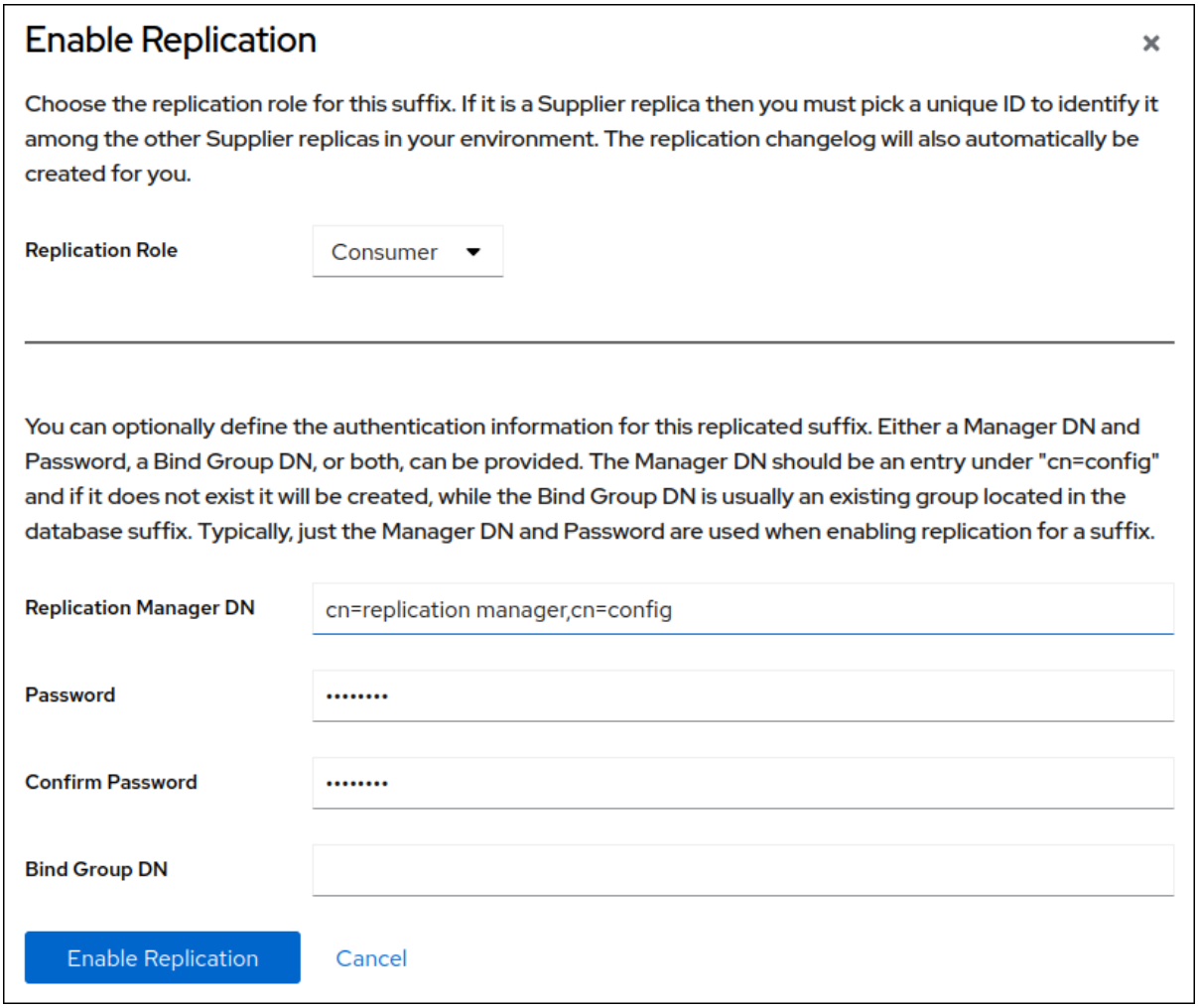
Perform this procedure on the consumer that you want to add to the replication topology.

Prerequisites

- You installed the Directory Server instance.
- The database for the **dc=example,dc=com** suffix exists.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Click **Enable Replication**.
4. Select **Consumer** in the **Replication Role** field, and enter the replication manager account and the password to create:



These settings configure the host as a consumer for the **dc=example,dc=com** suffix. Additionally, the server creates the **cn=replication manager,cn=config** user with the specified password and allows this account to replicate changes for the suffix to this host.

5. Click **Enable Replication**.

Verification

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. If the **Replica Role** field contains the value **Consumer**, replication is enabled, and the host is configured as a consumer.

Additional resources

- Installing Red Hat Directory Server
- Storing suffixes in separate databases

7.4. CONFIGURING THE HUB SERVER AS A SUPPLIER FOR THE CONSUMER USING THE WEB CONSOLE

To prepare the hub, you need to:

- Create a replication agreement to the consumer.
- Initialize the consumer.

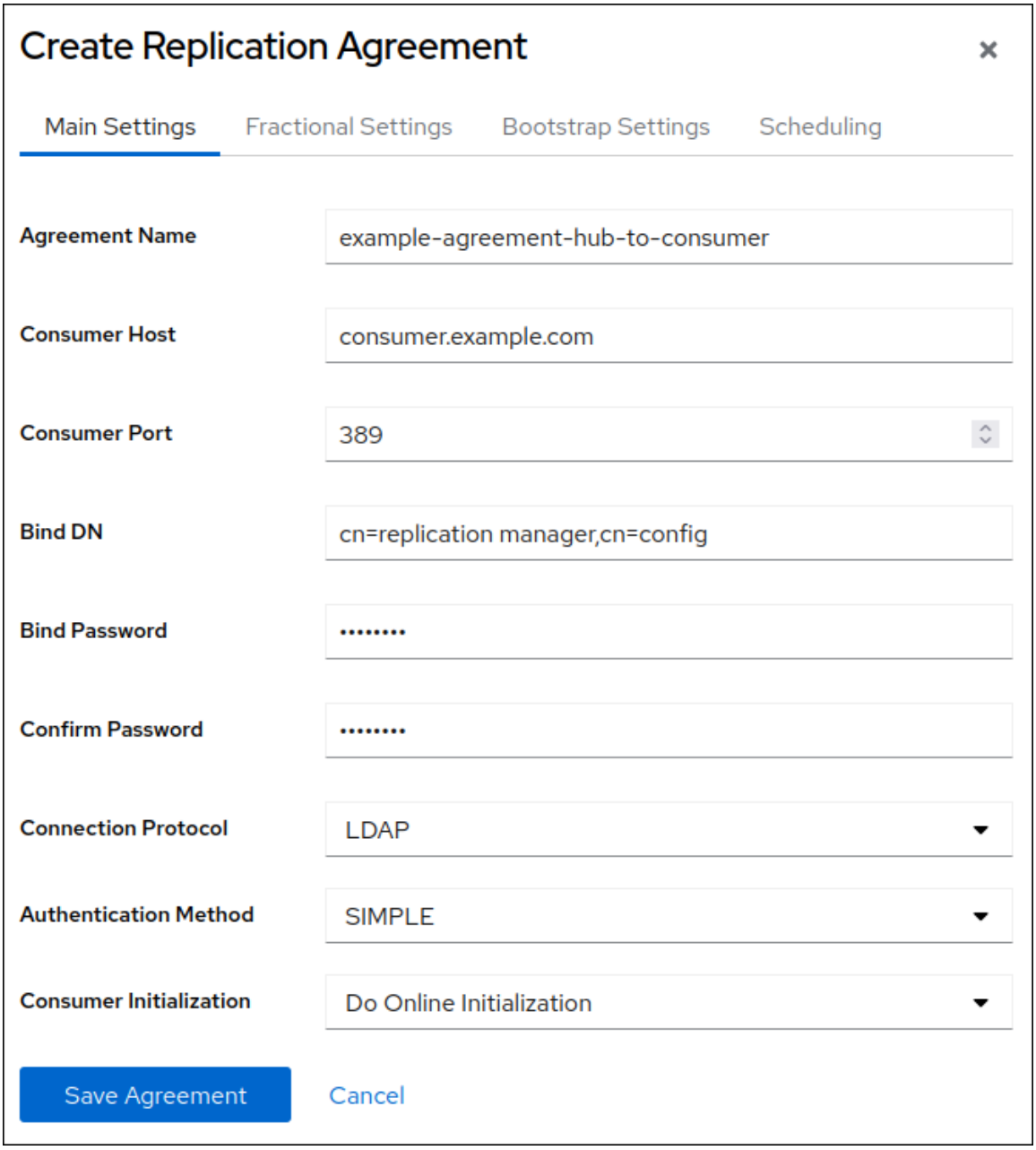
Perform this procedure on the hub in the replication topology.

Prerequisites

- The hub is initialized, and replication from the supplier to the hub works.
- You enabled replication for the dc=example,dc=com suffix on the hub.
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Add a replication agreement and initialize the consumer:
    a. On the **Agreements** tab, click **Create Agreement**, and fill the fields:



These settings create a replication agreement named **example-agreement-hub-to-consumer**. The replication agreement defines settings, such as the consumer's host name, protocol, and authentication information that the hub uses when connecting and replicating data to this consumer.

b. Select **Do Online Initialization** in the **Consumer Initialization** field to automatically initialize the consumer after saving the agreement.

c. Click **Save Agreement**.
After the agreement was created, Directory Server initializes **consumer.example.com**. Depending on the amount of data to replicate, initialization can be time-consuming.

Verification

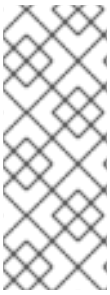
1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. On the **Agreements** tab, verify the status of the agreement in the **State** column of the table.


State
Last Init Status
Enabled
Initialized

CHAPTER 8. IMPROVING THE LATENCY IN A MULTI-SUPPLIER REPLICATION ENVIRONMENT

In certain multi-supplier replication environments, for example if the servers are connected over a wide area network (WAN), the replication latency can be high if multiple suppliers receive updates at the same time. This happens when one supplier exclusively accesses a replica without releasing it for a long time. In such situations, other suppliers cannot send updates to this consumer, which increases the replication latency.

To release a replica after a fixed amount of time, set the **nsds5ReplicaReleaseTimeout** parameter on suppliers and hubs.



NOTE

The **60** seconds default value is ideal for most environments. A value set too high or too low can have a negative impact on the replication performance. If you set the value too low, replication servers are constantly reacquiring each other, and servers are not able to send many updates. In a high-traffic replication environment, a longer timeout can improve situations where one supplier exclusively accesses a replica. However, in most cases, a value higher than **120** seconds slows down replication.

8.1. SETTING THE REPLICATION RELEASE TIMEOUT USING THE COMMAND LINE

To improve the replication efficiency in a multi-supplier replication environment, update the replication release timeout value on all hubs and suppliers.

Prerequisites

- You configured replication between multiple suppliers and hubs.

Procedure

1. Set the timeout value for the suffix:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication set --
suffix="dc=example,dc=com" --repl-release-timeout=70
```

   This command changes the replication timeout of the **example,dc=com** suffix to **70** seconds.

2. Restart the instance:

```
# dsctl instance_name restart
```

8.2. SETTING THE REPLICATION RELEASE TIMEOUT USING THE WEB CONSOLE

To improve the replication efficiency in a multi-supplier replication environment, update the replication release timeout value on all hubs and suppliers.

Prerequisites

- You configured replication between multiple suppliers and hubs.

Procedure

1. On the **Replication** tab, select the suffix entry.
2. Click **Show Advanced Settings**.
3. Update the value in the **Replication Release Timeout** field.
4. Click **Save Configuration**.

CHAPTER 9. REMOVING AN INSTANCE FROM A REPLICATION TOPOLOGY

In certain situations, such as hardware outages or structural changes, administrators want to remove Directory Server instances from a replication topology. The procedure of removing an instance depends on the role of the replica you want to remove.

9.1. REMOVING A CONSUMER OR HUB FROM A REPLICATION TOPOLOGY

If a consumer or hub is no longer needed in a replication topology, remove it.

Prerequisites

- The instance to remove is a consumer or hub.
- If the host to remove is a hub that also acts as a supplier to other servers in the topology, you configured other suppliers or hubs to replicate data to these servers to prevent them from becoming isolated.

Procedure

1. On the consumer or hub to remove:
   a. List the suffixes and their corresponding databases:

      ```
      # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend suffix list
      dc=example,dc=com (userroot)
      ```

      Note the name of the databases.

   b. Set the databases into read-only mode to prevent any further updates:

      ```
      # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend suffix set --enable-readonly "userroot"
      ```

2. On all suppliers that have a replication agreement with the consumer or hub you want to remove:
   a. List the replication agreements for the suffix that is replicated:

      ```
      # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt list --suffix "dc=example,dc=com"
      dn: cn=example-agreement,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
      cn: example-agreement
      ...
      ```

      The **cn** attribute contains the replication agreement name that you need in the next step.

   b. Remove the replication agreement:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt delete --suffix "dc=example,dc=com" example-agreement
```

3. On the consumer or hub to remove, disable replication for all suffixes:

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com replication disable --suffix "dc=example,dc=com"
```

If this host was a hub, disabling replication automatically also deletes all replication agreements for this suffix on this server.

Next steps

- If you want to use the removed instance for testing purposes, disable the read-only mode:

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend suffix set --disable-readonly userroot
```

IMPORTANT

If you want to use the instance you removed from the topology for testing purposes, ensure that no clients continue using it.

- Remove the instance:

```
# dsctl instance_name remove --do-it
```

Additional resources

- Configuring single-supplier replication using the command line
- Configuring multi-supplier replication using the command line
- Configuring cascading replication using the command line

9.2. REMOVING A SUPPLIER FROM A REPLICATION TOPOLOGY

Removing a supplier cleanly from a replication topology is more complex than removing a hub or consumer. This is because every supplier in the topology stores information about other suppliers, and they retain that information even if a supplier suddenly becomes unavailable.

Directory Server maintains information about the replication topology in a set of metadata called the replica update vector (RUV). The RUV contains information about the supplier, such as its ID, URL, latest change state number (CSN) on the local server, and the CSN of the first change. Both suppliers and consumers store RUV information, and they use it to control replication updates.

To remove a supplier cleanly, you must remove its metadata along with the configuration entries.

Prerequisites

- The instance to remove is a supplier.

- If the host to remove also acts as a supplier to other servers in the topology, you configured other suppliers or hubs to replicate data to these servers to prevent them from becoming isolated.

Procedure

1. On the supplier to remove:

   a. List the suffixes and their corresponding databases:

   ```
   # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
   suffix list
   dc=example,dc=com (userroot)
   ```

   Note the name of the databases.

   b. Set the databases into read-only mode to prevent any further updates:

   ```
   # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
   suffix set --enable-readonly "userroot"
   ```

   c. Wait until all other servers in the topology received all data from this supplier. To verify, ensure that the CSN on other servers is equal or greater than the CSN on the supplier to remove:

   ```
   # ds-replcheck online -D "cn=Directory Manager" -w password -m ldap://host-to-
   remove.example.com:389 -r ldap://server.example.com:389 -b dc=example,dc=com
   ================================================================================
   ========
           Replication Synchronization Report  (Tue Mar  5 09:46:20 2021)
   ================================================================================
   ========

   Database RUV's
   ==============================================

   Supplier RUV:
    {replica 1 ldap://host-to-remove.example.com:389} 5c7e8927000100010000
   5c7e89a0000100010000
    {replicageneration} 5c7e8927000000010000

   Replica RUV:
    {replica 1 ldap://host-to-remove.example.com:389} 5c7e8927000100010000
   5c7e8927000400010000
    {replica 2 ldap://server.example.com:389}
    {replicageneration} 5c7e8927000000010000
   ```

   d. Display the replica ID:

   ```
   # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com
   replication get --suffix "dc=example,dc=com" | grep -i "nsds5replicaid"
   nsDS5ReplicaId: 1
   ```

   In this example, the replica ID is **1**. Remember your replica ID for the last step of this procedure.

2. On all suppliers that have a replication agreement with the host you want to remove:

   a. List the replication agreements for the suffix that is replicated:

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt list --
   suffix "dc=example,dc=com"
   dn: cn=example-agreement,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
   tree,cn=config
   cn: example-agreement
   ...
   ```

   The **cn** attribute contains the replication agreement name that you need in the next step.

   b. Remove the replication agreement:

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt delete --
   suffix "dc=example,dc=com" example-agreement
   ```

3. On the supplier to remove, disable replication for all suffixes:

   ```
   # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com replication
   disable --suffix "dc=example,dc=com"
   ```

   Disabling replication automatically also deletes all replication agreements for this suffix on this server.

4. Before you proceed, ensure that all Directory Server instances listed in the **Replica RUV** section of the **ds-replcheck** output are online.

5. On one of the remaining suppliers in the topology, clean the RUVs for the replica ID:

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-tasks cleanallruv -
   -suffix "dc=example,dc=com" --replica-id 1
   ```

   This command requires that you specify the replica ID displayed in an earlier step of this procedure.

Verification

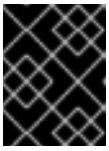
- Verify in the output of the **ds-replcheck** command that no entries with the replica ID and URL of the host you removed are left:

  ```
  # ds-replcheck online -D "cn=Directory Manager" -w password -m ldap://host-to-
  remove.example.com:389 -r ldap://server.example.com:389 -b dc=example,dc=com
  ```

Next steps

- If you want to use the removed instance for testing purposes, disable the read-only mode:

  ```
  # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
  suffix set --disable-readonly userroot
  ```



IMPORTANT

If you want to use the instance you removed from the topology for testing purposes, ensure that no clients continue using it.

- Remove the instance:

```
# dsctl instance_name remove --do-it
```

Additional resources

- Configuring single-supplier replication using the command line
- Configuring multi-supplier replication using the command line
- Configuring cascading replication using the command line

CHAPTER 10. PREVENTING MONOPOLIZATION OF A REPLICA IN A MULTI-SUPPLIER REPLICATION TOPOLOGY

In a multi-supplier replication topology, a supplier under heavy update load can monopolize a replica so that other suppliers are not able to update it as well.

This section describes the circumstances when monopolization happens, how to identify this problem, and provides information on how to configure suppliers to avoid monopolization situations.

10.1. WHEN MONOPOLIZATION HAPPENS

One of the features of multi-supplier replication is that a supplier acquires exclusive access to a replica. If the supplier attempts to acquire access while being locked out, the replica sends back a busy response, and the supplier waits for the time set in the **nsds5ReplicaBusyWaitTime** parameter before it starts another attempt. In the meantime, the supplier sends its update to another replica. When the first replica is free again, the supplier sends the updates to this host.

It can be a problem if the supplier that is locked out is under a heavy update load or has a lot of pending updates in the changelog. In this situation, the locking supplier finishes sending updates and immediately attempts to reacquire the same replica. Such an attempt succeeds in most cases, because other suppliers might still be waiting. You can set a pause between two update sessions in the **nsds5ReplicaSessionPauseTime** parameter. This can cause a single supplier to monopolize a replica for several hours or longer.

10.2. ENABLING REPLICATION LOGGING TO IDENTIFY MONOPOLIZATION OF REPLICAS

If one or more suppliers are often under a heavy update load, and replicas frequently do not receive updates, enable logging of replication messages to identify monopolization situations.

Prerequisites

- There are multiple suppliers in the replication topology.

Procedure

1. Enable replication logging:

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com config replace
   nsslapd-errorlog-level=8192
   ```

   Note that this command enables only replication logging, and logging other error messages is disabled.

2. Monitor the **/var/log/dirsrv/slapd-*instance_name*/errors** log file and search for the following error message:

   ```
   Replica Busy! Status: [Error (1) Replication error acquiring replica: replica busy]
   ```

   Note that it is normal if Directory Server occasionally logs this error. However, if replicas frequently do not receive updates, and the suppliers log this error, consider updating your configuration to solve this problem.

10.3. CONFIGURING SUPPLIERS TO AVOID MONOPOLIZATION OF REPLICAS

This procedure describes how to set parameters on a supplier to prevent monopolization of replicas.

Due to the differences of environments and load, set only the parameters that are relevant in your situation, and adjust the values according to your environment.

Prerequisites

- There are multiple suppliers in the replication topology.
- Directory Server frequently logs **Replica Busy! Status: [Error (1) Replication error acquiring replica: replica busy]** errors.

Procedure

1. Set the **nsds5ReplicaBusyWaitTime** parameter to configure the time a supplier waits before starting another attempt to acquire access to a replica after the replica sent a busy response:

   ```
   # dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt set --suffix "dc=example,dc=com" --busy-wait-time 5 replication_agreement_name
   ```

   This command sets the time to wait to **5** seconds. This setting applies only to the specified replication agreement.

2. Set the **nsds5ReplicaSessionPauseTime** parameter to configure the time a supplier waits between two update sessions:

   ```
   # dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt set --suffix "dc=example,dc=com" --session-pause-time 15 replication_agreement_name
   ```

   This command sets the pause to **15** seconds. By default, **nsds5ReplicaSessionPauseTime** is one second longer than the value in **nsds5ReplicaBusyWaitTime**. This setting applies only to the specified replication agreement.

3. Set the **nsds5ReplicaReleaseTimeout** parameter to terminate replication sessions after a given amount of time regardless of whether or not sending the update is complete:

   ```
   # dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication set --suffix "dc=example,dc=com" --repl-release-timeout 90
   ```

   This command sets the timeout to **90** seconds. This setting applies to all replication agreements for the specified suffix.

4. Optional: Set a timeout period for a supplier so that it does not stay connected to a consumer infinitely attempting to send updates over a slow or broken connection:

   ```
   # dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt set --conn-timeout 600 --suffix "dc=example,dc=com" replication_agreement_name
   ```

   This command sets the timeout to **600** seconds (10 minutes). To identify the optimum value, check the access log for the average amount of time the replication process takes, and set the timeout period accordingly.

Additional resources

- Configuration and schema reference

CHAPTER 11. FORCING REPLICATION UPDATES AFTER AN INSTANCE IN A REPLICATION ENVIRONMENT WAS OFFLINE

If you stop a Directory Server instance that is involved in replication for regular maintenance, the supplier must update the directory data immediately when it comes back online. You can enforce this update using the command line and the web console.

11.1. FORCING REPLICATION UPDATES USING THE COMMAND LINE

Perform the following steps on the suppliers to enforce replication updates for the **dc=example,dc=com** suffix in **example-agreement**.

Prerequisites

- The replication is set up.
- The consumer has been initialized.

Procedure

1. Check if the replication agreement has an update schedule configured:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt get --suffix "dc=example,dc=com" example-agreement
```

   If the output of the command contains **nsDS5ReplicaUpdateSchedule: *** or the **nsDS5ReplicaUpdateSchedule** parameter is not present, no update schedule is configured.

   If **nsDS5ReplicaUpdateSchedule** contains a schedule, such as shown in the following, note the value:

```
nsDS5ReplicaUpdateSchedule: 0800-2200 0246
```

2. If an update schedule is configured, enter the following command to temporary disable it:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt set --schedule \* --suffix "dc=example,dc=com" example-agreement
```

3. Temporarily disable the replication agreement:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt disable --suffix "dc=example,dc=com" example-agreement
```

4. Re-enable the replication agreement to force the replication update:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt enable --suffix "dc=example,dc=com" example-agreement
```

5. If a replication schedule was configured at the beginning of this procedure, set the schedule to the previous value:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt set --
schedule "0800-2200 0246" --suffix "dc=example,dc=com" example-agreement
```

Verification

- Display the replication status:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt status --
suffix "dc=example,dc=com" example-agreement
...
Last Update Start: 20210406120631Z
Last Update End: 20210406120631Z
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
...
```

11.2. FORCING REPLICATION UPDATES USING THE WEB CONSOLE

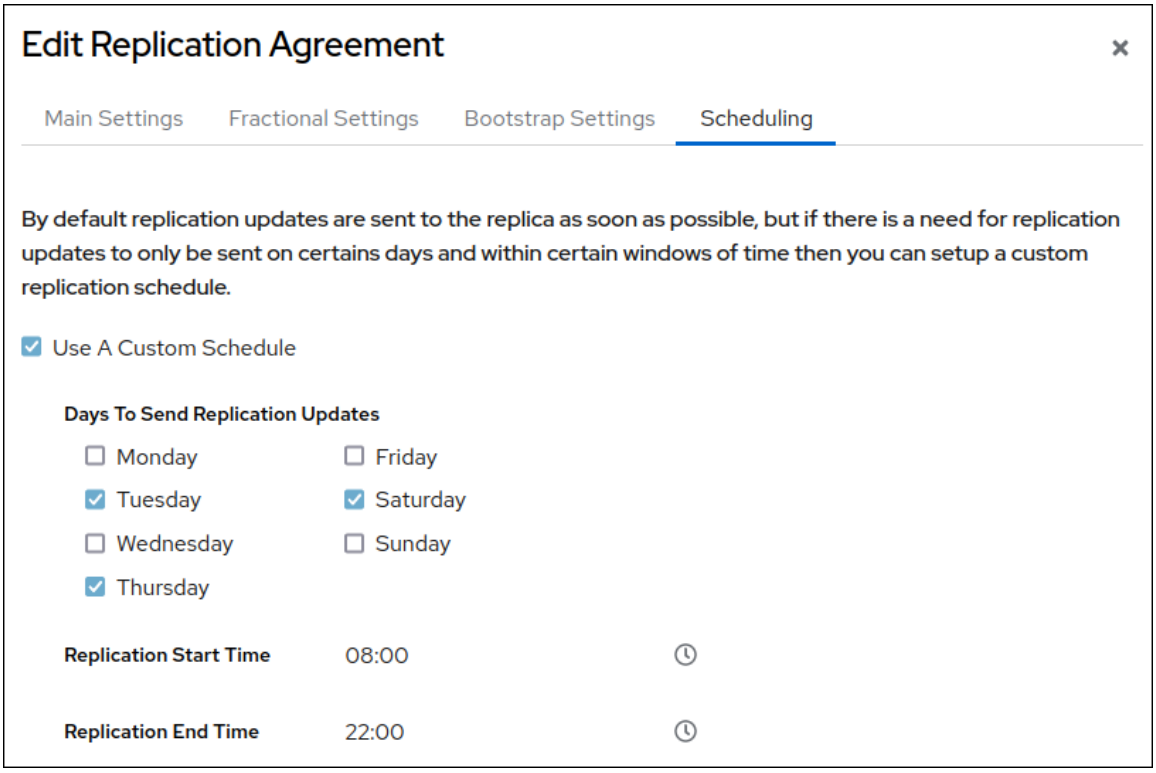
Perform the following steps on the suppliers to enforce replication updates.

Prerequisites

- The replication is set up.
- The consumer has been initialized
- You are logged in to the instance in the web console.

Procedure

1. Open the **Replication** menu.
2. Select the **dc=example,dc=com** suffix.
3. Open the **Agreements** tab.
4. Check if the replication agreement has an update schedule configured:
   a. Click the overflow menu next to the agreement, and select **Edit Agreement**.
   b. On the **Scheduling** tab, note the values that are currently set.



If **Use A Custom Schedule** is not selected, no schedule is configured.

5. Click the overflow menu next to the replication agreement, and select **Disable/Enable Agreement** to disable the agreement.
   The status of the agreement in the **State** column is now **Disabled**.

6. Click the overflow menu next to the replication agreement again, and select **Disable/Enable Agreement** to re-enable the replication agreement and enforce the replication update.
   The status of the agreement in the **State** column is now **Enabled**.

7. If a replication schedule was configured at the beginning of this procedure, set the schedule to the previous values:

   a. Click click the overflow menu, and select **Actions → Edit Agreement**.

   b. On the **Scheduling** tab, set the previous values.

Verification

- Display the replication status:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement
...
Last Update Start: 20210406120631Z
Last Update End: 20210406120631Z
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
...
```

CHAPTER 12. CHANGING THE ROLE OF A REPLICA

In a replication topology, you can change the role of replicas. For example, if a supplier is unavailable due to a hardware outage, you can promote a consumer to a supplier. The other way around, you can demote, for example, a supplier with low hardware resources to a consumer and later add another supplier with new hardware.

12.1. PROMOTING A REPLICA USING THE COMMAND LINE

You can promote:

- A consumer to a hub or supplier
- A hub to a supplier

This section describes how to promote a replica of the **dc=example,dc=com** suffix.

Prerequisites

- The Directory Server instance is a member of a replication topology.
- The replica to promote is a consumer or hub.

Procedure

1. If the replica to promote is a hub with replication agreements, and the hub should no longer send data to other hosts after the promotion, remove the replication agreements:
   a. List the replication agreements on the hub:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt list --suffix "dc=example,dc=com"
dn: cn=example-agreement,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
cn: example-agreement
...
```

   The **cn** attribute contains the replication agreement name that you need in the next step.

   b. Remove the replication agreement from the hub:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt delete --suffix "dc=example,dc=com" example-agreement
```

2. Promote the instance:
   - If you promote a consumer or hub to a supplier, enter:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication promote --suffix "dc=example,dc=com" --newrole "supplier" --replica-id 2
```

IMPORTANT

The replica ID must be a unique integer value between **1** and **65534** for a suffix across all suppliers in the topology.

- If you promote a consumer to a hub, enter:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication
promote --suffix "dc=example,dc=com" --newrole "hub"
```

3. If the replica in its new role should send updates to other hosts in the topology, create replication agreements.

Additional resources

- Configuring single-supplier replication using the command line
- Configuring multi-supplier replication using the command line
- Configuring cascading replication using the command line

12.2. PROMOTING A REPLICA USING THE WEB CONSOLE

You can promote:

- A consumer to a hub or supplier
- A hub to a supplier

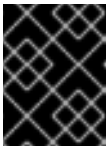
This section describes how to promote a replica of the **dc=example,dc=com** suffix.

Prerequisites

- The Directory Server instance is a member of a replication topology.
- The replica to promote is a consumer or hub.
- You are logged in to the instance in the web console.

Procedure

1. If the replica to promote is a hub with replication agreements, and the hub should no longer send data to other hosts after the promotion, remove the replication agreements:
   a. Navigate to **Replication → Agreements**.
   b. Click **Actions** next to the agreement you want to delete, and select **Delete Agreement**.
2. Navigate to **Replication → Configuration**, and click the **Change Role** button.
   - If you promote a consumer or hub to a supplier, select **Supplier**, and enter a unique replica ID.



IMPORTANT

The replica ID must be a unique integer value between **1** and **65534** for a suffix across all suppliers in the topology.

- If you promote a consumer to a hub, select **Hub**.

3. Select **Yes, I am sure**.
4. Click **Change Role**.
5. If the replica in its new role should send updates to other hosts in the topology, create replication agreements.

Additional resources

- Configuring single-supplier replication using the web console
- Configuring multi-supplier replication using the web console
- Configuring cascading replication using the web console

12.3. DEMOTING A REPLICA USING THE COMMAND LINE

You can demote:

- A supplier or hub to a consumer
- A hub to a consumer

This section describes how to demote a replica of the **dc=example,dc=com** suffix.

Prerequisites

- The Directory Server instance is a member of a replication topology.
- The replica to demote is a supplier or hub.

Procedure

1. If the replica to demote has replication agreements that are no longer needed, for example, because you demote the replica to a consumer, remove the replication agreements:
   a. List the replication agreements on the replica:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt list --suffix "dc=example,dc=com"
dn: cn=example-agreement,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
cn: example-agreement
...
```

   The **cn** attribute contains the replication agreement name that you need in the next step.

   b. Remove the replication agreement from the replica:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt delete --
suffix "dc=example,dc=com" example-agreement
```

2. Demote the instance:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication demote --
suffix "dc=example,dc=com" --newrole "hub_or_consumer"
```

   Depending on the role you want to configure, set the **--newrole** parameter to **hub** or **consumer**.

3. If you configured the replica as a hub and it should send updates to other hosts in the topology, create replication agreements.

Additional resources

- Configuring single-supplier replication using the command line
- Configuring multi-supplier replication using the command line
- Configuring cascading replication using the command line

12.4. DEMOTING A REPLICA USING THE WEB CONSOLE

You can demote:

- A supplier or hub to a consumer
- A hub to a consumer

This section describes how to demote a replica of the **dc=example,dc=com** suffix.

Prerequisites

- The Directory Server instance is a member of a replication topology.
- The replica to demote is a supplier or hub.
- You are logged in to the instance in the web console.

Procedure

1. If the replica to demote has replication agreements that are no longer needed, for example, because you demote the replica to a consumer, remove the replication agreements:
   a. Navigate to **Replication → Agreements**.
   b. Click **Actions** next to the agreement you want to delete, and select **Delete Agreement**.
2. Navigate to **Replication → Configuration**, and click **Change Role** button.
3. Select the new replica role.
4. Select **Yes, I am sure**.

5. Click **Change Role**.

6. If the replica in its new role should send updates to other hosts in the topology, create replication agreements.

Additional resources

- Configuring single-supplier replication using the web console
- Configuring multi-supplier replication using the web console
- Configuring cascading replication using the web console

CHAPTER 13. TRIMMING THE REPLICATION CHANGELOG

The Directory Server changelog manages a list of received and processed changes. It includes client changes and changes received from replication partners.

By default, Directory Server trims the changelog entries that are older than seven day. However, you can configure:

- A maximum age of entries in the changelog in the **nsslapd-changelogmaxage** parameter.
- The total number of records in the changelog in the **nsslapd-changelogmaxentries** parameter.

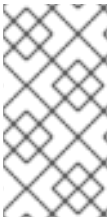
If you enabled at least one of these settings, Directory Server trims the changelog every five minutes by default (**nsslapd-changelogtrim-interval**).

Even with the trimming settings enabled, any record and records subsequently created remain in the changelog until they are successfully replicated to all servers in the topology. If you remove the supplier from the topology as described in Removing a supplier from a replication topology , then Directory Server trims all the updates of this supplier from changelogs on other servers.

13.1. CONFIGURING REPLICATION CHANGELOG TRIMMING USING THE COMMAND LINE

Directory Server trims the changelog entries that are older than seven days by default. However, you can configure the time after which Directory Server removes entries. You can also configure Directory Server to automatically remove entries if the number of entries exceeds a configured value.

This section describes how to configure changelog trimming for the **dc=example,dc=com** suffix.



NOTE

Red Hat recommends setting a maximum age instead of a maximum number of entries. The maximum age should match the replication purge delay set in the **nsDS5ReplicaPurgeDelay** parameter in the **cn=replica,cn=suffixDN,cn=mapping tree,cn=config** entry.

Perform this procedure on the supplier.

Prerequisites

- You enabled replication for the **dc=example,dc=com** suffix.

Procedure

1. Configure change log trimming:
   - To set a maximum age of changelog entries, enter:

     ```
     # dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --suffix "dc=example,dc=com" --max-age "4w"
     ```

     This command sets the maximum age to 4 weeks. The parameter supports the following units:

- **s** (**S**) for seconds
- **m** (**M**) for minutes
- **h** (**H**) for hours
- **d** (**D**) for days
- **w** (**W**) for weeks

- To set a maximum number of entries, enter:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --suffix "dc=example,dc=com" --max-entries "100000"
```

This command sets the maximum number of entries in the changelog to 100,000.

2. By default, Directory Server trims the changelog every 5 minutes (300 seconds). To set a different interval, enter:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --suffix "dc=example,dc=com" --trim-interval 600
```

This command sets the interval to 10 minutes (600 seconds).

Verification

- Display the changelog settings of the suffix:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication get-changelog --suffix "dc=example,dc=com"
dn: cn=changelog,cn=userroot,cn=ldbm database,cn=plugins,cn=config
cn: changelog
nsslapd-changelogmaxage: 4w
nsslapd-changelogtrim-interval: 600
...
```

The command only displays the parameters that are different to their default.

13.2. MANUALLY REDUCING THE SIZE OF A LARGE CHANGELOG

In certain situations, such as if replication changelog trimming was not enabled, the changelog can grow to an excessively large size. To fix this, you can reduce the changelog size manually.

This procedure describes how to trim the changelog of the **dc=example,dc=com** suffix. Perform this procedure on the supplier.

Prerequisites

- You enabled replication for the **dc=example,dc=com** suffix.

Procedure

1. Optional: Display the size of the changelog:

a. Identify the back-end database of the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backend suffix list
dc=example,dc=com (userroot)
```

The name in parentheses is the back-end database that stores the data of the corresponding suffix.

b. Display the size of the changelog file of the **userroot** backend:

```
# ls -lh /var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db
-rw-------. 1 dirsrv dirsrv 517M Jul  5 12:58
/var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db
```

2. To be able to reset the parameters after reducing the changelog size, display and note the current values of the corresponding parameters:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication get-
changelog --suffix "dc=example,dc=com"
dn: cn=changelog,cn=userroot,cn=ldbm database,cn=plugins,cn=config
cn: changelog
nsslapd-changelogmaxage: 4w
nsslapd-changelogtrim-interval: 300
```

If you do not see any specific attributes in the output, Directory Server uses their default values.

3. Temporarily, reduce trimming-related parameters:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-
changelog --suffix "dc=example,dc=com" --max-age "300s" --max-entries 500 --trim-
interval 60
```

IMPORTANT

For performance reasons, do not permanently use too short interval settings.

4. Wait until the time set in the **--trim-interval** parameter expires.

5. Compact the changelog to regain disk space:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backend compact-db --
only-changelog
```

6. Reset the changelog parameters to the values they had before you temporarily reduced them:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-
changelog --suffix "dc=example,dc=com" --max-age "4w" --trim-interval 300
```

Verification

- Display the size of the changelog:

```
# ls -lh /var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db
-rw-------. 1 dirsrv dirsrv 12M Jul  5 12:58
/var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db
```

CHAPTER 14. ENCRYPTING THE REPLICATION CHANGELOG

Encrypt the replication changelog to increase the security of your instance, in case that an attacker gains access to the file system of your server.

Changelog encryption uses the server's TLS encryption key and the same PIN to unlock the key. You must either enter the PIN manually upon server startup or use a PIN file.

Directory Server uses randomly generated symmetric cipher keys to encrypt and decrypt the changelog. The server uses a separate key for each configured cipher. These keys are wrapped using the public key from the server's TLS certificate, and the resulting wrapped key is stored within the server's configuration files. The effective strength of the attribute encryption is the same as the strength of the server's TLS key used for wrapping. Without access to the server's private key and the PIN, it is not possible to recover the symmetric keys from the wrapped copies.

14.1. ENCRYPTING THE CHANGELOG USING THE COMMAND LINE

To increase the security in a replication topology, encrypt the changelog on suppliers and hubs. This procedure describes how to enable changelog encryption for the **dc=example,dc=com** suffix.

Prerequisites

- The server has TLS encryption enabled.
- The host is a supplier or hub in a replication topology.

Procedure

1. Export the changelog, for example, to the **/tmp/changelog.ldif** file:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication export-changelog to-ldif -o /tmp/changelog.ldif -r "dc=example,dc=com"
```

2. Enable change log encryption for the **dc=example,dc=com** suffix:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication --suffix "dc=example,dc=com" --encrypt
```

3. Import the changelog from the **/tmp/changelog.ldif** file:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication import-changelog from-ldif -r "dc=example,dc=com" /tmp/changelog.ldif
```

4. Restart the instance:

```
# dsctl instance_name restart
```

Verification

1. Make a change in the LDAP directory, such as updating an entry.
2. Stop the instance:

```
# dsctl instance_name stop
```

3. List the suffixes and their corresponding databases:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backend suffix list
dc=example,dc=com (userroot)
```

Note the name of the database for which you enabled changelog encryption.

4. Enter the following command to display parts of the changelog:

```
# dbscan -f /var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db |
tail -50
```

If the changelog is encrypted, you see only encrypted data.

5. Start the instance.

```
# dsctl instance_name start
```

Additional resources

- Enabling TLS-encrypted connections to Directory Server

CHAPTER 15. TROUBLESHOOTING REPLICATION-RELATED PROBLEMS

This section lists frequent error messages in replication environments, explains possible causes, and offers remedy.

15.1. CONFIGURING DIRECTORY SERVER TO LOG REPLICATION-RELATED ERRORS

To log replication-related errors, enable replication debugging. The **nsslapd-errorlog-level** parameter is additive. This means that, to enable multiple logging features, you have to add the values of each logging feature, and set the sum in **nsslapd-errorlog-level**.

Procedure

1. Display the current error log level:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-errorlog-level
nsslapd-errorlog-level: 16384
```

2. The value to enable replication debugging is **8192**. Set the **nsslapd-errorlog-level** parameter to **24576** (**8192** + the previous value **16384**) to enable replication debugging in addition to the currently enabled error logging features:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-errorlog-level=24576
```

15.2. OVERVIEW OF REPLICATION-RELATED ERRORS, CAUSES, AND POSSIBLE SOLUTIONS

The following is an overview of replication-related errors and possible solutions:

agmt=*agreement_name* (*host_name*:*port*) Replica has a different generation ID than the local data

- Reason: The consumer specified in parenthesis of the message has not been successfully initialized yet, or it was initialized from a different root supplier.
- Impact: The local supplier will not replicate any data to the consumer.
- Solution: Ignore this message if it occurs before the consumer is initialized. Otherwise, reinitialize the consumer if the message is persistent. In a multi-supplier environment, all servers need be initialized only once from a root supplier, directly or indirectly. For example, server **S1** initializes **S2** and **S4**, **S2** then initializes **S3**, and so on. The important thing to note is that **S2** must not start initializing **S3** until the initialization of **S2** is done. For this, check the total update status from the web console on **S1** or in the error log of **S1** or **S2**. Also, **S2** should not initialize **S1** back.

Warning: data for replica's was reloaded, and it no longer matches the data in the changelog. Recreating the changelog file. This could affect replication with replica's consumers, in which case the consumers should be reinitialized.

- Reason: This message can appear only when you restart a supplier. It indicates that the supplier was unable to write the changelog or did not flush out its replica update vector (RUV) at its last shutdown. The former case usually happens because of a disk-space problem, and the latter case because a server crashed or was ungracefully shut down.

- Impact: The server is not be able to send the changes to a consumer if the consumer's **maxcsn** value no longer exists in the server's changelog.

- Remedy: Check the disk space and for possible core files under the server's logs directory. If this is a single-supplier replication, reinitialize the consumers. Otherwise, if the server later complains that it cannot locate change sequence numbers (CSN) for a consumer, verify if the consumer can receive the CSN from other suppliers. If not, reinitialize the consumer.

Too much time skew

- Reason: The system clocks on the host machines are extremely out of sync.

- Impact: Directory Server uses the system clock to generate a part of the CSN. In order to reflect the change sequence among multiple suppliers, suppliers would forward-adjust their local clocks based on the remote clocks of the other suppliers. Because the adjustment is limited to a certain amount, any difference that exceeds the permitted limit will cause the replication session to be aborted.

- Remedy: Synchronize the system clocks on the Directory Server host machines, for example, by configuring the **chronyd** service.

agmt=*agreement_name* (*host_name*:*port*): Warning: Unable to send endReplication extended operation (*error_message*)

- Reason: The consumer is not responding.

- Impact: If the consumer recovers without being restarted, there is a chance that the replica on the consumer will be locked forever if it did not receive the release lock message from the supplier.

- Remedy: Watch if the consumer can receive any new change from any of its suppliers, or start the replication monitor, and see if all the suppliers of this consumer warn that the replica is busy. If the replica appears to be locked forever and no supplier can get in, restart the consumer.

Changelog is getting too big.

- Reason: Either changelog purge is turned off, which is the default setting, or changelog purge is turned on, but some consumers are way behind the supplier.

- Remedy: By default, changelog purge is turned off. To turn it on from the command line, enter:

  ```
  # dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --max-age 1d --suffix "dc=example,dc=com"
  ```

  1d means 1 day. Other valid time units are **s** for seconds, **m** for minutes, **h** for hours, and **w** for weeks. A value of **0** turns off the purge.

  With changelog purge turned on, a purge thread that wakes up every five minutes removes a change if its age is greater than the value you set and if it has been replayed to all the direct consumers of this supplier or hub.

If it appears that the changelog is not purged when the purge threshold is reached, check the maximum time lag from the replication monitor among all the consumers. Irrespective of what the purge threshold is, no change will be purged before it is replayed by all the consumers.

CHAPTER 16. MONITORING THE REPLICATION TOPOLOGY USING THE COMMAND LINE

To monitor the state of the directory data replication between suppliers, consumers, and hubs, you can use replication topology report that provides information on the replication progress, replica IDs, number of changes, and other parameters. To generate the report faster and make it more readable, you can configure your own credentials and aliases.

16.1. DISPLAYING A REPLICATION TOPOLOGY REPORT USING THE COMMAND LINE

To view overall information about the replication status for each agreement in your replication topology, you can display the replication topology report. To do so, use the **dsconf replication monitor** command.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.

Procedure

- To view a replication topology report, enter:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication monitor
```

The **dsconf** utility will request authentication credentials for each instance in the topology:

```
Enter password for cn=Directory Manager on ldap://supplier.example.com: password
Enter a bind DN for consumer.example.com:389: cn=Directory Manager
Enter a password for cn=Directory Manager on consumer.example.com:389: password

Supplier: server.example.com:389
--------------------------------
Replica Root: dc=example,dc=com
Replica ID: 1
Replica Status: Online
Max CSN: 5e3acb77001d00010000

Status For Agreement: "example-agreement" (consumer.example.com:1389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20211209122116Z
Last Update End: 20211209122116Z
Number Of Changes Sent: 1:21/0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20211209122111Z
Last Init End: 20211209122114Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: In Synchronization
```

```
Replication Lag Time: 00:00:00

Supplier: consumer.example.com:1389
---------------------------------
Replica Root: dc=example,dc=com
Replica ID: 65535
Replica Status: Online
Max CSN: 00000000000000000000
```

Additional resources

- Setting credentials for replication monitoring in the .dsrc file
- Using aliases in the replication topology monitoring output
- Displaying a replication topology report using the web console

16.2. SETTING CREDENTIALS FOR REPLICATION MONITORING IN THE .DSRC FILE

By default, the **dsconf replication monitor** command asks for bind DNs and passwords when authenticating to remote instances. To generate the report faster and easier in the future, you can set the bind DNs, and optionally passwords, for each server in the topology in the user's ~/**.dsrc** file.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.

Procedure

1. Optional: Create the ~/**.dsrc** file.
2. In the ~/**.dsrc** file, set the bind DNs, and passwords. For example:

```
[repl-monitor-connections]
connection1 = server1.example.com:389:cn=Directory Manager:*
connection2 = server2.example.com:389:cn=Directory Manager:[~/pwd.txt]
connection3 = hub1.example.com:389:cn=Directory Manager:S3cret
```

This example uses connection1 to connection3 as keys for each entry. However, you can use any unique key.

When you run the **dsconf replication monitor** command, the **dsconf** utility connects to all servers configured in replication agreements of the instance. If the utility finds the hostname in ~/**.dsrc**, it uses the defined credentials to authenticate to the remote server. In the example above, **dsconf** uses the following credentials when connecting to a server:

Hostname	Bind DN	Password setup method
server1.example.com	cn=Directory Manager	Requests the password

Hostname	Bind DN	Password setup method
server2.example.com	cn=Directory Manager	Reads the password from **~/pwd.txt**
hub1.example.com	cn=Directory Manager	S3cret

Verification

- Run the **dsconf replication monitor** command to see If **dsconf** utility uses credentials configured in the ~/**.dsrc** file. For more information, see Displaying a replication topology report using the command line.

Additional resources

- Setting credentials for replication monitoring using the web console

16.3. USING ALIASES IN THE REPLICATION TOPOLOGY MONITORING OUTPUT

To make the report more readable, you can set your own aliases that will be displayed in the report output. By default, the replication monitoring report contains the hostnames of remote servers.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.

Procedure

If you want to see aliases in the report, use one of the following methods:

- Define the aliases in the ~/**.dsrc** file:

```
[repl-monitor-aliases]
M1 = server1.example.com:389
M2 = server2.example.com:389
```

- Define the aliases by passing the **-a alias=*host_name:port*** parameter to the **dsconf replication monitor** command:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication monitor -a
M1=server1.example.com:389 M2=server2.example.com:389
```

In both cases, the **dsconf replication monitor** command displays the alias in the output:

```
...
Supplier: M1 (server1.example.com:389)
--------------------------------
```

```
Replica Root: dc=example,dc=com

...
Supplier: M2 (server2.example.com:389)
--------------------------------
Replica Root: dc=example,dc=com
```

Additional resources

- Configuring replication naming aliases using the web console

CHAPTER 17. MONITORING THE REPLICATION TOPOLOGY USING THE WEB CONSOLE

To monitor the state of the directory data replication between suppliers, consumers, and hubs, you can use replication topology report that provides information on the replication progress, replica IDs, number of changes, and other parameters. To generate the report faster and make it more readable, you can configure your own credentials and aliases.

17.1. DISPLAYING A REPLICATION TOPOLOGY REPORT USING THE WEB CONSOLE

To view overall information about the replication status for each agreement in your replication topology, you can display the replication topology report.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.
- You are logged in to the web console.

Procedure

1. Navigate to **Monitoring → Replication**. The **Replication Monitoring** page opens.
2. Click **Generate Report**.
3. Enter the passwords for login to remote instances and click **Confirm Credentials Input**.
   Directory Server uses bind DNs values from existing replication agreements.
   The replication topology report will be generated on the **Report Result** tab.

NOTE

To generate another replication topology report, go to the **Prepare Report** tab.

Additional resources

- Setting credentials for replication monitoring using the web console
- Configuring replication naming aliases using the web console
- Displaying a replication topology report using the command line

17.2. SETTING CREDENTIALS FOR REPLICATION MONITORING USING THE WEB CONSOLE

To generate the replication topology report faster and easier, you can set your own bind DNs, and optionally passwords, for each server in the topology for authentication. In this case, you do not need to confirm replication credentials each time you want to generate a replication topology report. By default, Directory Server takes these credentials from existing replication agreements.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumer.
- You are logged in to the web console.

Procedure

1. Navigate to **Monitoring → Replication**. The **Replication Monitoring** page opens.
2. Click **Add Credentials**.
3. Enter replication login credentials you want to use for authentication to remote instances:
   - **Hostname**. A remote instance hostname you want the server to authenticate to.
   - **Port**. A remote instance port.
   - **Bind DN**. Bind DN used for authentication to the remote instance.
   - **Password**. A password used for authentication.
   - **Interactive Input**. If checked, Directory Server will ask for a password every time you generate a replication topology report.
4. Click **Save**.

Verification

Generate the replication topology report to see If the report asks for the credentials. For more information, see Displaying a replication topology report using the web console .

17.3. CONFIGURING REPLICATION NAMING ALIASES USING THE WEB CONSOLE

To make the report more readable, you can set your own aliases that will be displayed in the report output. By default, the replication monitoring report contains the hostnames of servers.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.
- You are logged in to the web console.

Procedure

1. Navigate to **Monitoring → Replication**. The **Replication Monitoring** page opens.
2. Click **Add Alias**.
3. Enter alias details:
   - **Alias**. An alias that will be displayed in the replication topology report.

- **Hostname**. An instance hostname.
- **Port**. An instance port.

4. Click **Save**.

Verification

- Generate the replication topology report to see If the report uses new aliases. For more information, see Displaying a replication topology report using the web console .

CHAPTER 18. COMPARING TWO DIRECTORY SERVER INSTANCES

You can verify that two Directory Server instances are synchronized using **ds-replcheck** utility. You can compare two servers either online or using two LDIF-formatted files in offline mode.

18.1. DISPLAYING THE REPLICATION STATUS OF TWO DIRECTORY SERVER INSTANCES

You can use the **ds-replcheck** utility to display the replication status of two Directory Server instances.

Procedure

- Use the following command to display the replication status of two Directory Server instances:

```
# ds-replcheck state -D "cn=Directory Manager" -W -m ldap://server1.example.com:389
-r ldap://server2.example.com:389 -b "dc=example,dc=com"
Replication State: Replica is behind Supplier by: 264 seconds
```

18.2. COMPARING TWO ONLINE DIRECTORY SERVER INSTANCES

If you compare two online servers, the contents of the databases usually differ, if they are under heavy load. To work around this problem, the **ds-replcheck** uses a lag time value by passing the **-l *time_in_seconds*** parameter to **ds-replcheck**. By default, this value is set to **300** seconds (5 minutes). If the utility detects an inconsistency that is within the lag time, the utility does not report it. This helps to reduce false positives.

By default, if you have excluded certain attributes in the replication agreement from being replicated, **ds-replcheck** reports these attributes as different. To ignore these attributes, pass the **-i *attribute_list*** parameter to the utility.

Procedure

- To compare the **dc=example,dc=com** suffix of **supplier.example.com** and **replica.example.com** online, enter:

```
# ds-replcheck online -D "cn=Directory Manager" -W -m
ldap://supplier.example.com:389 -r ldap://replica.example.com:389 -b
"dc=example,dc=com"
```

  The **-m** and **-r** parameters set the URLs to the supplier and replica.

18.3. COMPARING OFFLINE TWO DIRECTORY SERVER INSTANCES

To compare two offline Directory Server instances, export the databases on both hosts and compare them using **ds-replcheck**.

By default, if you have excluded certain attributes in the replication agreement from being replicated, **ds-replcheck** reports these attributes as different. To ignore these attributes, pass the **-i *attribute_list*** parameter to the utility.

Procedure

1. On the supplier, list the suffixes and their corresponding databases:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com backend suffix list
dc=example,dc=com (userroot)
o=test (test_database)
```

   Note the name or suffix of the database you want to compare.

2. Export the database while the instance is running:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com backend export -r -l
/var/lib/dirsrv/slapd-instance_name/ldif/export-supplier.ldif userRoot
```

   The **-r** parameter ensures that the export includes replication state information, and **-l** sets the path to the export file. Note that the **dirsrv** user must have write permissions in the destination directory to create that file.

3. Repeat the previous steps on the replica you want to compare with the supplier.

4. Copy the exported file from one host to the other. For example, to copy the LDIF file from **replica.example.com** to **supplier.example.com**, enter the following command on the replica:

```
# scp /var/lib/dirsrv/slapd-instance_name/ldif/export-replica.ldif
supplier.example.com:/var/lib/dirsrv/slapd-instance_name/ldif/
```

   Note that this command requires that you can access the supplier using SSH.

5. On the supplier, compare the two LDIF files:

```
# ds-replcheck offline -m /var/lib/dirsrv/slapd-instance_name/ldif/export-supplier.ldif -r
/var/lib/dirsrv/slapd-instance_name/ldif/export-replica.ldif -rid 1 -b
"dc=example,dc=com"
```

   The **-m** and **-r** parameters set the paths to the supplier and replica, and **-rid** sets the replica identifier of the supplier.

18.4. EXPLANATION OF THE DS-REPLCHECK OUTPUT

The output of the **ds-replcheck** utility contains the following sections:

Database RUV's

Lists the Replication Update Vectors (RUV) of the databases including the minimum and maximum Change Sequence Numbers (CSN). For example:

```
Supplier RUV:
 {replica 1 ldap://supplier.example.com:389} 58e53b92000200010000 58e6ab46000000010000
 {replica 2 ldap://replica.example.com:389} 58e53baa000000020000 58e69d7e000000020000
 {replicageneration} 58e53b7a000000010000

Replica RUV:
 {replica 1 ldap://supplier.example.com:389} 58e53ba1000000010000 58e6ab46000000010000
 {replica 2 ldap://replica.example.com:389} 58e53baa000000020000 58e7e8a3000000020000
 {replicageneration} 58e53b7a000000010000
```

Entry Count

Displays the total number of entries on the both servers, including tombstone entries. For example:

```
Supplier:  12
Replica: 10
```

Tombstones

Displays the number of tombstone entries on each replica. These entries are added to the total entry count. For example:

```
Supplier:  4
Replica: 2
```

Conflict Entries

Lists the Distinguished Names (DN) of each conflict entry, the conflict type, and the date it was created. For example:

```
Supplier Conflict Entries: 1

 - nsuniqueid=48177227-2ab611e7-afcb801a-ecef6d49+uid=user1,dc=example,dc=com
   - Conflict:   namingConflict (add) uid=user1,dc=example,dc=com
   - Glue entry: no
   - Created:    Wed Apr 26 20:27:40 2021


Replica Conflict Entries: 1

 - nsuniqueid=48177227-2ab611e7-afcb801a-ecef6d49+uid=user1,dc=example,dc=com
   - Conflict:   namingConflict (add) uid=user1,dc=example,dc=com
   - Glue entry: no
   - Created:    Wed Apr 26 20:27:40 2021
```

Missing Entries

Lists the DNs of each missing entry and the creation date from the other server where the entry resides. For example:

```
Entries missing on Supplier:
 - uid=user2,dc=example,dc=com (Created on Replica at: Wed Apr 12 14:43:24 2021)
 - uid=user3,dc=example,dc=com (Created on Replica at: Wed Apr 12 14:43:24 2021)

Entries missing on Replica:
 - uid=user4,dc=example,dc=com (Created on Supplier at: Wed Apr 12 14:43:24 2021)
```

Entry Inconsistencies

Lists the DNs of the entry that contain attributes that are different to those on the other server. If a state information is available, it is also displayed. If no state information for an attribute is available, it is listed as an origin value. This means that the value was not updated since the replication was initialized for the first time. For example:

```
cn=group1,dc=example,dc=com
---------------------------
Replica missing attribute "objectclass":
```

```
- Supplier's State Info: objectClass;vucsn-58e53baa000000020000: top
- Date: Wed Apr  5 14:47:06 2021

- Supplier's State Info: objectClass;vucsn-58e53baa000000020000: groupofuniquenames
- Date: Wed Apr  5 14:47:06 2021
```

CHAPTER 19. SOLVING COMMON REPLICATION PROBLEMS

Multi-supplier replication uses an eventually-consistency replication model. This means that the same entries can be changed on different servers. When replication occurs between these two servers, Directory Server needs to resolve the conflicting changes. Mostly, resolution occurs automatically, based on the timestamp associated with the change on each server. The most recent change has priority. However, there are some cases where conflicts require manual intervention in order to reach a resolution.

19.1. IDENTIFYING AND SOLVING NAMING CONFLICTS

When several supplier servers receive a request to create an entry with the same distinguished name (DN), each server creates the entry with this DN and a different entry unique identifier (entry ID). The entry ID is stored in the **nsuniqueid** operational attribute.

For example, **Server A** and **Server B** receive a request to create **uid=*user_name*,ou=people,dc=example,dc=com** user entry. As a result, each server has its own entry:

- On Server A, the entry has:
  - **uid=*user_name*,ou=people,dc=example,dc=com**
  - **nsuniqueid=a7f1758b-512211ec-b115e2e9-7dc2d46b**
- On Server B, the entry has:
  - **uid=*user_name*,ou=people,dc=example,dc=com**
  - **nsuniqueid=643a461e-b61311e1-b23be826-4afeed5f**

During replication, **Server A** replicates newly created entry **uid=*user_name*,ou=people,dc=example,dc=com** to **Server B**, and **Server B** replicates newly created entry to **Server A**, and a naming conflict occurs on each server. By comparing change sequence numbers (CSN), each server determines which entry was created earlier. For example, the entry on **Server B** was created earlier.

The automatic conflict resolution procedure changes the last entry created (the entry on **Server A**) the following way:

- Adds the **nsuniqueid** value to the non-unique DN.
- Adds the **nsds5replconflict** attribute with the description which operation caused the conflict.
- Adds the **ldapsubentry** objectclass.

Now the following entries exist on both servers:

- The **valid** entry with:
  - **uid=user_name,ou=people,dc=example,dc=com**
  - **nsuniqueid=643a461e-b61311e1-b23be826-4afeed5f**
- The **conflict** entry with:
  - **nsuniqueid=a7f1758b-512211ec-b115e2e9-7dc2d46b+uid=user_name,ou=people,dc=example,dc=com**

- **nsuniqueid=a7f1758b-512211ec-b115e2e9-7dc2d46b**

To solve the naming conflict manually, use the following procedure on each server.

Procedure

1. List the conflict entries:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict list
dc=example,dc=com
dn: nsuniqueid=a7f1758b-512211ec-b115e2e9-
7dc2d46b+uid=user_name,ou=people,dc=example,dc=com
cn: user_name
displayName: user
gidNumber: 99998
homeDirectory: /var/empty
legalName: user name
loginShell: /bin/false
nsds5replconflict: namingConflict (ADD)
uid=user_name,ou=people,dc=example,dc=com
objectClass: top
objectClass: nsPerson
objectClass: nsAccount
objectClass: nsOrgPerson
objectClass: posixAccount
objectClass: ldapsubentry
uid: user_name
uidNumber: 99998
```

2. If conflict entries exist, decide how to proceed:

   - To keep only the valid entry (**uid=user_name,ou=people,dc=example,dc=com**) and delete the conflict entry, enter:

     ```
     # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict delete
     nsuniqueid=a7f1758b-512211ec-b115e2e9-
     7dc2d46b+uid=user_name,ou=People,dc=example,dc=com
     ```

   - To keep only the conflict entry (**nsuniqueid=a7f1758b-512211ec-b115e2e9-7dc2d46b+uid=user_name,ou=People,dc=example,dc=com**) and delete the valid entry, enter:

     ```
     # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict swap
     nsuniqueid=a7f1758b-512211ec-b115e2e9-
     7dc2d46b+uid=user_name,ou=People,dc=example,dc=com
     ```

   - To keep both entries, specify a new relative distinguished name (RDN) to rename the conflict entry:

     ```
     # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict
     convert --new-rdn=uid=user_name_NEW nsuniqueid=a7f1758b-512211ec-
     b115e2e9-7dc2d46b+uid=user_name,ou=people,dc=example,dc=com
     ```

     This command renames the conflict entry to **uid=user_name_NEW,ou=people,dc=example,dc=com**.

WARNING

Directory Server replicates LDAP operations performed on a conflict entry. Usually replicated operations target the entry by using the **nsuniqueid** of the original operation entry rather than by using the operation **dn**. However, in cases with conflict entries, the behavior might differ.

19.2. IDENTIFYING AND SOLVING ORPHAN ENTRY CONFLICTS

When Directory Server replicates a delete operation and the consumer server finds that the entry to be deleted has child entries, the conflict resolution procedure creates a glue entry to avoid having orphaned entries in the directory.

In the same way, when Directory Server replicates an add operation and the consumer server cannot find the parent entry, the conflict resolution procedure creates a glue entry for the parent.

Glue entries are temporary entries that include the object classes **glue** and **extensibleObject**. Glue entries can be created in several ways:

- If the conflict resolution procedure finds a deleted entry with a matching unique identifier, the glue entry has the same attributes as the deleted entry, but with the added **glue** object class and the **nsds5ReplConflict** attribute.
  In such cases, either modify the glue entry to remove the **glue** object class and the **nsds5ReplConflict** attribute to keep the entry as a normal entry or delete the glue entry and its child entries.

- The server creates an entry with the **glue** and **extensibleObject** object classes.

Procedure

1. List the orphan entry conflicts:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict list-glue suffix
dn: ou=parent,dc=example,dc=com
objectClass: top
objectClass: organizationalunit
objectClass: glue
objectClass: extensibleobject
ou: parent
```

2. If orphan entry conflicts exist, decide how to proceed:

   - To delete a glue entry and its child entries, enter:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict delete-glue "ou=parent,dc=example,dc=com"
dn: ou=parent,dc=example,dc=com
objectClass: top
```

```
objectClass: organizationalunit
objectClass: extensibleobject
ou: parent
```

- To convert a glue entry into a regular entry, enter:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict
convert-glue "ou=parent,dc=example,dc=com"
```

19.3. IDENTIFYING AND SOLVING ERRORS ABOUT OBSOLETE OR MISSING SUPPLIERS

Directory Server stores information about the replication topology, such as all suppliers that send updates to other replicas, in a set of metadata called replica update vector (RUV). An RUV contains information about the supplier, such as its ID and URL, the last change state number (CSN) on the local server, and the CSN of the first change. Both suppliers and consumers store RUV information, and they use it to control replication updates.

When you remove a supplier from the replication topology, information about it can remain in another replica's RUV. You can use a **cleanallruv** task to remove the RUV entry form all suppliers in the topology.

Prerequisites

- Replication is enabled on.

Procedure

1. Monitor the **/var/log/dirsrv/slapd-*instance_name*/errors** log file and search for entries similar to the following:

```
[22/Jan/2021:17:16:01 -0500] NSMMReplicationPlugin - ruv_compare_ruv: RUV [changelog
max RUV] does not contain element [{replica 8 ldap://server2.example.com:389}
4aac3e59000000080000 4c6f2a02000000080000] which is present in RUV [database RUV]
...
[22/Jan/2021:17:16:01 -0500] NSMMReplicationPlugin - replica_check_for_data_reload:
Warning: for replica dc=example,dc=com there were some differences between the
changelog max RUV and the database RUV. If there are obsolete elements in the database
RUV, you should remove them using the CLEANALLRUV task. If they are not obsolete, you
should check their status to see why there are no changes from those servers in the
changelog.
```

   In this case, the replica ID **8** causes this error.

2. Display all RUV records and replica IDs, both valid and invalid:

```
# dsconf -D "cn=Directory Manager" ldap://server1.example.com replication get-ruv --
suffix "dc=example,dc=com"
RUV:        {replica 1 ldap://server1.example.com} 61a4d8f8000100010000
61a4f5b8000000010000

Replica ID: 1
LDAP URL:   ldap://server1.example.com
Min CSN:    2021-11-29 13:43:20 1 0 (61a4d8f8000100010000)
Max CSN:    2021-11-29 15:46:00 (61a4f5b8000000010000)
```

```
RUV:        {replica 2 ldap://server2.example.com} 61a4d8fb000100020000
61a4f550000000020000

Replica ID: 2
LDAP URL:   ldap://server2.example.com
Min CSN:    2021-11-29 13:43:23 1 0 (61a4d8fb000100020000)
Max CSN:    2021-11-29 15:44:16 (61a4f550000000020000)
 RUV:       {replica 8 ldap://server3.example.com} 61a4d903000100080000
61a4d908000000080000

Replica ID: 8
LDAP URL:   ldap://server3.example.com
Min CSN:    2021-11-29 13:43:31 1 0 (61a4d903000100080000)
Max CSN:    2021-11-29 13:43:36 (61a4d908000000080000)
```

Note the list of returned replica IDs: **1**, **2**, and **8**.

3. Run cleanup tasks for the replica IDs **8**.

```
# dsconf -D "cn=Directory Manager" ldap://server1.example.com repl-tasks cleanallruv
--suffix="dc=example,dc=com" --replica-id=8
```

Note that Directory Server replicates RUV cleanup tasks. Therefore, you need to start the tasks on only one supplier.

If one of the replicas can not be joined, for example if it is down, you can use the **--force-cleaning** option to achieve an immediate clean up of the RUV.

Verification

- Display the RUV records and replica IDs:

```
# dsconf -D "cn=Directory Manager" ldap://server1.example.com replication get-ruv --
suffix "dc=example,dc=com"
RUV:        {replica 1 ldap://server1.example.com} 61a4d8f8000100010000
61a4f5b8000000010000

Replica ID: 1
LDAP URL:   ldap://server1.example.com
Min CSN:    2021-11-29 14:02:10 1 0 (61a4d8f8000100010000)
Max CSN:    2021-11-29 16:00:00 (61a4f5b8000000010000)
RUV:        {replica 2 ldap://server2.example.com} 61a4d8fb000100020000
61a4f550000000020000

Replica ID: 2
LDAP URL:   ldap://server2.example.com
Min CSN:    2021-11-29 14:02:10 1 0 (61a4d8fb000100020000)
Max CSN:    2021-11-29 15:58:22 (61a4f550000000020000)
```

The command no longer returns RUV entries for the replica IDs **8**.